

安全保障上の電子的監視

——権力分立と合衆国憲法修正第四条の交錯

富井幸雄

故長内了本学名誉教授に捧ぐ

一 はじめに—アメリカ憲法と諜報

1 諜報 (intelligence) への関心

2 合衆国憲法修正第四条への関心

3 本稿の目的と構成

二 電子的監視と修正第四条—刑事司法での展開

1 修正第四条の古典的意義

2 電子盗聴と修正第四条のその後の展開

3 Title III (タイトル・スリー)

4 小 括

安全保障上の電子的監視 (富井)

三 安全保障の電子的監視と修正第四条

1 問題の所在

2 Keith 判決

3 Keith 法理の課題

4 外国諜報監視法 (FISA) の制定

四 安全保障捜査の電子的監視のコンプレックス―修正第四条の守備範囲と権力分立

1 プライバシー―空間の限定

2 特別の必要性の法理

3 権力分立と修正第四条

五 国家安全保障局 (NSA) の電子的監視と修正第四条

1 NSA による電子的監視とその現状

2 NSA の組織と法

3 NSA による電子的監視の違憲性

4 小 括

六 むすびにかえて

小手先の安全を得るために、必須の自由を諦めることができる人々は、自由にも安全にもあずかることはない。^(一) “They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety”.

一 はじめに—アメリカ憲法と諜報

1 諜報 (intelligence) への関心

アメリカは九・一一同時多発テロ（以下九・一一）以降、安全保障の重点をテロ対策に置き、国土安全保障省（Department of Homeland Security (DHS)）を設置するなど、組織の強化も含めて、その実効を期している。アルカイダなどの国際テロ組織への対策である。しかし、二〇一三年四月のボストン・マラソンでのテロは、いわゆる自前のテロの恐怖を見せつけ、国内のテロからの安全保障に一石を投じている。

外国に対する諜報活動 (foreign intelligence) は九・一一前から、一九七八年制定の外国諜報監視法 (Foreign Intelligence Surveillance Act (FISA) 50 U.S.C. §1801 et seq.) に基づいて行われている。ここに来て国内での諜報活動がさかんととなり、NSA (National Security Agency 国家安全保障局) をはじめ、FBI (Federal Bureau of Investigation 連邦捜査局) やCIA (Central Intelligence Agency 中央諜報局) といった諜報機関が、隠密にアメリカ国民のEメールや電話の通信記録、インターネットの記録などを収集するようになっていた。これを暴露したNSAの契約職員E. Snowdenの事件は記憶に新しい⁽³⁾。社会保障を充実させる福祉国家は個人の情報を必要とする。安全保障国家も同様で、高度に発達したテクノロジーを利用しながら、アメリカは監視国家になっていった⁽⁴⁾。安全保障のための電子的監視（本稿では電話盗聴からインターネットを含む通信の傍受を含む）がテロ対策に有効なツールとして多用されるようになっていた。

安全保障目的で情報を秘密裏に収集することを諜報 (intelligence) と観念する⁽⁵⁾。「外国の権力や組織、人やそのエー

ジェントの活動、能力、計画、意図についての時宜を得た正確な情報は、合衆国の安全保障に不可欠である」(EO (Executive Order 大統領命令) 12333)。もっとも、対テロを中心に安全保障を構築するとき、その標的は海外に限定されるわけではなく、国内のアメリカ市民にも向けられることとなる。国内育ちのテロリストを警戒するのだ。⁽⁶⁾

諜報は刑事捜査とは一線を画する。諜報を法執行機関に行わせるのは、かつてのカナダのように珍しくはない。⁽⁷⁾ F B Iは法執行と諜報の両方を行っている。R・ボズナーは、九・一一後のアメリカの諜報機関のあり方を考察した著書で、諜報について次のようにまとめている。⁽⁸⁾「諜報の目的は潜在的な敵の意図と能力を学ぶことである。：諜報においては、データはスパイによって、新聞雑誌、ウェブや科学技術雑誌といった公に利用できる資料を渉猟することによって、そして、イメージや信号の諜報といったテクノロジーの監視手段によって、収集される。データは照合解釈のために分析官に与えられ、その分析の結果は政策責任の官吏に送られる。かくして、収集、分析、行動の、三つのレベルが存在する。行動は、諜報で明らかになったことに従って行動する権限を付与された官吏による、分析への対応である」。

アメリカは、九・一一を含む安全保障上の危機の経験を経ながら、現在、連邦政府に一七の諜報機関を擁し、諜報共同体 (Intelligence Community (IC)) を形成している。EO 12333 (50 U.S.C. § 401a (4)) では以下の機関とされる。The Office of the Director of National Intelligence (国家諜報長官局) 、Air Force, Army, Marine Corps, Navy Intelligence Units (陸海空軍海兵隊各諜報室) 、C I A、Coast Guard Intelligence (沿岸警備隊諜報部) 、Defense Intelligence Agency (incl. National Intelligence Centers) (国防諜報庁) 、Office of Intelligence, Department of Energy (エネルギー省諜報部) 、Office of Intelligence and Analysis, Department of Homeland Security (国土安全保障省諜報分析部) 、Bureau of

Intelligence and Research, Department of State (国務省諜報調査局)・Office of Intelligence and Analysis, Department of Treasury (財務省諜報分析部)・Office of National Security Intelligence, Drug Enforcement Administration (DEA) (麻薬取締庁安全保障課報部)・National Security Branch, Federal Bureau of Investigation (FBI) (連邦捜査局安全保障支局)・National Geospatial-Intelligence Agency (NGA) (国家地政課報庁)・National Reconnaissance Office (NRO) (国家偵察局)・NSA。これらは、国家諜報組織、国防省組織、軍務諜報組織、文民諜報組織の四つのカテゴリーに分類される。⁽⁹⁾ 国家諜報組織は、CIA、NSA、NRO、NGAである。⁽¹⁰⁾

こうしたICを総轄するのが、二〇〇四年の諜報改革テロ防止法 (Intelligence Reform and Terrorism Prevention Act (IRTPA)) で設置されたDNI (Director of National Intelligence 国家諜報長官) である。これは九・一一委員会の報告を反映させている。しかし、諜報機関の改革は終わったわけではなく、諜報活動の効率性や統制のための議論はいまだ止んでいない。⁽¹¹⁾ ICの一七もの官僚機構をどう束ねるかは、DNIの権限も絡んで困難な問題である。⁽¹²⁾ あわせて二〇万人前後の職員を擁し、七五億ドル規模 (二〇一二年度 (FY2012) では五三億九千万ドル) の予算を費やす諜報機関で、⁽¹³⁾ 統合や過剰問題が常にとり沙汰され、諜報の重複など効率性は予算では必ず議論される。⁽¹⁴⁾

そもそも、諜報は国家活動として認められるか。アメリカ合衆国憲法 (以下憲法) に諜報や秘密の情報収集の規定はない。しかし、外国の諜報をなすのは憲法上黙示の必要な政府権限だとの認識は、以下のような前提から共有される。⁽¹⁵⁾ 第一に、諜報が安全保障にとって不可欠であること。第二に、諜報の果実は、技術が結果を出せば出すほど、意思決定者にとって重要性が増していくこと。第三に、秘密の諜報活動は執行権によって管理されなければならないこと。第四に、アメリカ憲法はいかなる作用も大統領に独占を許さず、諜報の責務にあっても議会と共有されなければならない

ならないこと、である⁽¹⁶⁾。

大統領は、「道理が示す限り諜報の業務をアレンジすることができる（フェデラリスト・ペーパー第六四篇）。フェデラリストの「^{ジュイ}」は条約締結に関して、こう述べる。「条約の交渉において、性質がいかようであれ、完全な秘密と即時の処理が必須であることはおうおうにしてあることだ。それらは、最も有益な諜報が、それを保持している人が、それが公にされる懸念から解放されるなら、獲得できる場合である。そうした懸念は温情的か友好的かのいずれかの動機に駆り立てられて、そうした人に作用することとなる。まぎれもなく、大統領の秘密に頼るけれども、上院のそれには信頼を置かず、いわんや大所帯の人民議会のそれにおいておやとする、両方に動機づけられた人が多く存在する。『大統領は上院の助言と承認に基づいて条約を締結するが』、それにもかかわらず、彼は道理が示唆するようなやりかたで、諜報の業務を管理できる⁽¹⁷⁾」。条約締結を典型とする安全保障には迅速と秘密が要求される⁽¹⁸⁾。それには執行権が最も適任であるとの認識だ。諜報という国家の事務が権力分立上執行権の作用であるとの認識は、はやばやと確立されたといつてよからう。

2 合衆国憲法修正第四条への関心

一方で、諜報にはプライバシー侵害が懸念される。憲法は公権力の私生活への介入には、修正第四条で次のように規定して、制限している。「人民がその身体、家宅、書類その他物件を不合理な搜索や押収（unreasonable searches and seizures）から保全される権利は侵害されてはならず、しかも宣誓あるいは確約に基づく相当な理由（probable cause）に基づき、かつ、押収されるべき身体あるいは物と搜索されるべき場所を個別具体的に記載していなければ、

令状は発給されてはならない」。

同条は、軍の私人宅での宿営 (quartering) を制限した修正第三条の直後に置かれているように、⁽¹⁹⁾ イギリスの特に軍の暴挙を糾弾する意味で設けられ、個人の居宅、そして財産に、公権力は勝手に侵入してはならないことを意図した。自分の家は自分の城 (His house is his own castle) とのコモンロー原則に基づき、自分の私的空間、特に財産は不可侵との思想を表している。⁽²⁰⁾ 不合理な搜索押収から個人の城が守られる、そしてそこに侵入するには令状が必要である、との法は、イングランドの経験に基づく。⁽²¹⁾ 修正第四条は、刑事手続において、犯罪を行ったと信ずるに足る相当な理由 (probable cause) があって、それを司法裁判所が判断し (実体的制約)、なおかつ、これらのことを明記した令状によらなければ (手続的制約)、搜索や押収 (search and seizure) はされないとする法である。

修正第四条は、文言上明らかに、人民に保全される権利を保障している。保全されるものは、個人の身体、家宅、書類、その他の物件であり、公権力の不当な搜索や押収から保護されるとする。公権力は刑事司法の利益を図らなければならないから、この権利を侵害できるけれども、その場合は搜索や押収の必要性を示す合理的な実体的理由がなければならない、加えて、その対象となる物を特定して記載した司法官憲の令状を要するとした。

修正第三条が保護される領域を個人の家宅としたのに対し、修正第四条にはそうした限定的な文言はなく、広がりをもっている。同条は搜索押収には、令状と相当な理由を要請し、両者を欠く証拠を排除する (exclusionary rule) 趣旨である。⁽²²⁾ 刑事手続では証拠となる物品等の押収や会話の聴取といった、いわば特定された物 (後にみるように有体物のみではなく会話等も入るとされる) が必要であり、したがって令状にはこれを特定した記載が、憲法上要求される。一方、安全保障のための情報収集や諜報は、特定のではなく、あるいは特定できないし、極秘になされることを旨とす

る。アメリカ人がテロリストと交信するのを傍受するのに、同条に基づいて令状を要するのか。諜報のこうした特殊性を考えたとき、刑事手続と同様に司法権の前にさらけ出して、相当の理由を弁明させ、どのような令状を要するするのか。

アメリカは安全保障のための諜報活動を秘密裏に行ってきた⁽²³⁾。これが世論を喚起させ、一九七〇年代に議会はいわゆるチャーチ委員会をたちあげ、これまでのCIAをはじめとする政府の諜報活動をすべて暴露して、課題を洗い出した⁽²⁴⁾。これをうけて、諜報活動に透明性をもたせて統制するために、一九七八年にFISAが制定される。同法によって、外国の政府や機関と外国人に対して、そのアメリカでの交信記録を収集できる。スノーデンが明らかにしたNSAの活動では、司法的なプロセスもなく無令状で、かつ諜報機関の判断のみで、個人のEメールを含む電信記録が収集されたり、電子盗聴(eavesdropping)されたりするようになっていた。それは、二〇〇八年にFISAが改正されるまでは、EO 12333でなされていた⁽²⁵⁾。安全保障上の監視は、通常の司法警察上の監視とは別に扱われる⁽²⁶⁾。

修正第四条は刑事司法に手続的制約を設けたのであり、安全保障のための情報収集(諜報)は語っていない。同条が諜報活動にも及ぶかが議論となる。ここで留意したいのは、安全保障には大統領の専権が憲法上認められ、それは大統領固有の権限であって、議会等の関与は受けないといった、権力分立の問題が絡むことである⁽²⁷⁾。

安全保障のための外国諜報の法的基準は、二つのベクトルのせめぎ合いのなかで定立される⁽²⁸⁾。一つは、アメリカ国内でなされる以上、刑事司法での盗聴と同視すべきで、修正第四条を完全に適用させるとするものである。もう一つは、安全保障には大統領に特別の権限が認められており、同条の射程外でなされうるとするものである。安全保障の情報収集での電子的監視は、実に憲法の権力分立と人権保障が複雑にクロスした問題なのである。

諜報機関が安全保障目的で収集した証拠で刑事訴追できるかは問題となる。⁽²⁹⁾これが認められると、司法が全く関与しないで盗聴がなされ、そこで得られた証拠で刑事訴追されることになり、修正第四条からは想像できない状況が生まれることになる。後にみるように、連邦最高裁判所（以下最高裁）の判例をうけて、議会は刑事訴追のための盗聴について立法（Title III of the Omnibus Control and Safe Streets Act of 1968, 18 U.S.C. § 2510 et seq.）を設け、司法の令状による電子的監視を認めている。その一〇年後、やはり最高裁の判例をうけてFISAを制定し、海外での外国政府間に限定された交信の諜報の電子的監視を法務長官の判断（ただしFISA裁判所（後述）の同意が原則必要）で広く行えるようにした。

テロをはじめ予測不可能で重篤な被害をもたらす犯罪あるいは安全保障上の事犯を未然に防ぐことは、安全保障上のプライオリティである。そこでは効率的に、秘密裏に情報を収集することが国家利益となる。一方で、個人のプライバシーも重要な利益であり、刑事手続では修正第四条が公権力の刑事司法上の利益にこれを優先させた。安全保障についてどうなのかが、ここでの問題である。九・一一以降、安全保障の利益のために修正第四条を考慮しない扱いを拡大させる方向もみられる。⁽³⁰⁾

3 本稿の目的と構成

本稿は、安全保障が憲法の人権保障の利益と衝突する深刻な局面にメスを入れる。テクノロジーの発展に裏打ちされて、諜報活動としての電子的監視（electronic surveillance）に、憲法、とくに修正第四条が適用されるのか、されどすれほどのように関係するのかを検討する。

まず修正第四条の意義と問題点を、次の二点を明らかにすることで、明確にする。第一に、修正第四条が電子的監視をどのように考えてきたのかの判例の推移をみる。修正第四条制定時、よもや電子的監視とか盗聴とかは想像だにされていなかった。しかし、テクノロジーの急速な発展は、現在も高度に発達していく電子的監視の手法を生み出している。同条は、テクノロジーの進展と緊張関係にたつ典型的な憲法条項である。それは、プライバシーという憲法上保護された人権と衝突する。そこで第二に、同条はプライバシーをどのように理解したのかについて、判例の変遷をみる。修正第四条はプライバシーの根拠となる条項である。こうした議論は、同条の直接のターゲットである刑事司法手続の空間で展開されてきた。同条は刑事手続の規定であり、その際盗聴について同条の適用除外が認められることがあるのか、判例をうけて立法でどう整理されたのかも、観察する。

そのうえで、本稿の主題に入る。すなわち、安全保障に修正第四条が厳格に適用されるのかを検討する。NSAは国民の知らぬところで諜報としての電子的監視を行っていることが明らかとなった。判例は、以下みていくように、電子空間は解放された空間でプライバシーの及ぶところではないとしており、立法も、安全保障のために執行権たる諜報機関の便宜で電子盗聴や第三者からの情報提供（安全保障請求状（National Security Letters (NSLs)）など）を用意している。こうした状況では「修正第四条は死文化（dead letter）した」ともいわれる。⁽³²⁾なるほど安全保障の諜報は歴史的には古くから大統領の専権領域とされ、議会の関与はなかった。しかし、一九七二年の最高裁判決（*Katz*）を契機に、CIAなどの秘密の諜報活動が国内の反政府運動家にも向けられていたことが暴露されたのも手伝って、この領域での民主的アカウンタビリティが志向されるようになる。そこでFISAを制定し、外国権力の諜報に立法的根拠を与えた。そのプロセスが事後に議会へ報告する以外は執行権で進められることから、二〇一三年に問題となった

ような国内諜報活動の電子的監視にチェックが入らない現象が生じる。九・一一以降、こうした諜報活動は諜報機関の整備や改編、さらに権限付与の拡大で深刻になっているのである。

アメリカではテロ対策が深刻になるなか、安全保障の名目で、諜報機関による国内での諜報活動、とくにEメールや電話の通信などの情報収集を執行権の判断のみでなすようになっていく。かかる活動の有用性は否定しうるものではないけれども、憲法の人権保障との関係でどうバランスをとるべきかは慎重を要する。⁽³³⁾ 諜報にあつては、おりから対テロでびりびりしている状況下では、大統領の安全保障権限よろしく、NSAが暗躍するようになり、彼らの判断のみで無令状でサイバー空間を監視するようになれば、修正第四条とまともにぶつかることになる。⁽³⁴⁾ 対テロの電子的監視の令状は、政府機関にテロの諜報、つまり将来のテロ事犯を防止し伝統的な搜索令状のような特別の刑事的に絞られた証拠を要求しない情報の収集を授權する。⁽³⁵⁾ 安全保障が絡めば軍の諜報活動も浸潤していくのであり、これをどうチェックするかも問題となろう。⁽³⁶⁾ テロのような深刻な安全保障事案からわれわれはのがれられない以上、人権保障と安全保障のバランスは注意深く考察せねばならない。

電子的監視は、修正第四条制定時には考えだにされなかった。しかし、テクノロジーは民間のみならず公権力組織にも、他者を監視するのに使用されるようになってくる。監視(surveillance)は、スロボギンにならつて、「人の情報を離れたところから、通常密かに私的空間に侵入することなしに収集する政府の努力」と観念しておく。⁽³⁷⁾ それには三類型ある。第一は通信監視(communications surveillance)で、リアルタイムに通信を傍受する。第二は物理的監視(physical surveillance)で、リアルタイムに物理的活動を観察する。第三が取引監視(transaction surveillance)で、通信、活動その他の取引について記録された情報にアクセスするのを含む。政府の諜報は長くこれらに依存してきた

が、九・一一以降安全保障のための監視に最新のテクノロジーを使用して、場末に至るまで広範に実施されるようになったという。とりわけ後二者が重用されるようになる。⁽³⁸⁾ 高度に発達した、そして日々進歩する通信テクノロジーに、一八世紀に制定された修正第四条がどう対応しようとするのかを垣間見ることとなる。

二 電子的監視と修正第四条—刑事司法での展開

修正第四条は刑事手続における公権力抑制のルールである。その趣意は文言上明らかで、個人の私生活領域は恣意的な刑事司法権力の名の下では侵されず、正当な理由のある官憲の発する令状に基づいてのみ、その侵害が正当化される。これすなわち、刑事司法での搜索押収には令状が必要とする規範である。しかし、個人の支配領域がテクノロジーの発展で通信の空間にまで広がり、プライバシーが顔を出すようになってくるとき、⁽³⁹⁾ この原則を時勢にどう適合させていくのが、同条の課題として突き付けられることとなる。

1 修正第四条の古典的意義

修正第四条を制定したとき、制憲者はよもや電話が世間に流布し、ましてや電子で通信が自由にできるとは考えておるまい。同条で想定していたのは、公権力が物理的に (physically) 勝手に私人のテリトリーに入ってくることであった。ほとんどの州に修正第四条と同様な規定が設けられるようになった一七八九年に、アメリカはコモローの伝統の中に搜索押収に関して最も広範な制約を建設した。⁽⁴⁰⁾ その後、テクノロジーの発達で、私人の領域が電子的空間

にまで広がりをもせた。それは当事者間の秘密の領域であるから、犯罪の相談もなされよう。制定から一〇〇年ほどは、同条の保護領域について論争がなかったけれども、電話の普及によってにわかに問題が認識されるようになる。以後、修正第四条の展開は技術の発達に同条をどう適合させていくかが軸となる。⁽⁴¹⁾

電話盗聴は、禁酒法 (National Prohibition Act) が制定されてかかる捜査手法がとられるようになると、憲法問題が提起されるようになる。一九二八年、私人間の電話の会話を傍受できるかが問題となったとき、修正第四条との関係が意識された。禁酒法違反で、ワシントン州シアトルの警察が被告人の事務所の電話を約五か月間盗聴し、その証拠を刑事裁判に持ちだしたことで、この盗聴は修正第四条 (第五条違反も主張したが、第四条のみ判断) に違反すると訴えた。最高裁は、制憲者は電話を想定しておらず、同条の保護は被告人の家や事務所から全世界に到達する電線にまで及ぶとは想定されず、電線傍受は彼の家や事務所の侵入ではないとした (Orin ^{オリン} ^{ステッド} ^{事件} ⁽⁴²⁾)。すなわち、同条で保護されるのは、同条が列記しているような有体物 (tangible objects) であり、それが保全されるのは物理的な侵害 (physical invasion) からであって、本件電話傍受はこれに当たらない (no physical intrusion) したのである。修正第四条の文言にこたわり、物理的な次元で保障を捉えた。

これにたいし ^{ブランドス} Brandes 判事は、多数意見は文理にとらわれ、同条が禁じた手法あるいは手続に留意していないとして、反対意見を述べている。⁽⁴³⁾ 一人に放っておいてもらう権利、つまりプライバシーの権利は、文明社会で最も価値があり、「この権利を保護するために、いかなる手段によろうとも、個人のプライバシーに政府が不当に侵入することとは、修正第四条違反とみなされる」。⁽⁴⁴⁾ 制憲時、政府には「むき出しの実力 (force and violence)」で強制できる手段しかなかったが、テクノロジーの発達により、繊細なやり方で個人の領域に入ることができるようになった。そもそも

制憲者は、「アメリカ人の信条、思想、感情や情緒を保護する」ことを意図した。そのため、政府から放っておいてもらう権利、プライバシーが最も重要だとされたのであって、いかなる手段であれ、これを侵害する政府の不当な行為は同条に違反するとした。⁽⁴⁵⁾

多数意見はプライバシーの概念を持ち出さず、盗聴した場所（事務所から道路に出ている電話線に傍受装置を仕掛けた）は彼の財産ではないとし、同条が保護しているのは財産の不可侵だと認識した。ブランドイスは、そうした物権的有体物のみが対象ではないとした。彼が一八八九年にハーバード法学雑誌に出した古典的論文「プライバシー権」⁽⁴⁶⁾よりしく、同条が保護しようとしたのは個人の私的領域といったプライバシーなのだとしたのである。その後、プライバシーの議論は修正第四条に端を発して、同条で保護されるかどうかで議論されるようになっていく。⁽⁴⁷⁾

修正第四条はもう一つの重要な原理を規定している。令状主義である。実体的に保護される個人の財産や身体の保全を規定するとともに、これらを刑事司法のために差押えるには、判事の令状が必要だとして、手続の原理を据えたのである。「修正第四条のポイントは、それが、合理的な人が証拠から導き出す通常の推論を支持することを法執行官に否定することにあるのではない。その保護は、そうした推論がしばしば犯罪を探し出す競合した企てに従事する官吏によって判断される代わりに、つながりのない中立の司法官憲（magistrate）⁽⁴⁸⁾によって導き出されなければならない」とすることにある」。修正第四条は、刑事司法において個人の財産を侵害する時は合理的な理由を要し、それが司法官憲の令状によって担保される憲法原理を明確にしたのである。

2 電子盗聴と修正第四条のその後の展開

テクノロジーの発展に、修正第四条の原則を適合させていくとともに、判例をうけて立法で対応していった。制憲者は電子盗聴なるものは想定していなかった。科学技術の進歩は想定外だった。電話盗聴という新たな政府の手法には、一九三四年に連邦交信法 (Federal Communication Act) を制定し、「電話の同定の情報へのアクセスあるいは交信傍受を実効化するには適切な授權」(§605) を求めなければならないとの手続を確立させるように、一般通信事業者に義務づけた。⁽⁴⁹⁾ いわく、「なんぴとも送り手が認めない限り、電子交信を傍受し、いかなる者とのそうした傍受された交信の存在と、内容と、実体と趣旨と、または意味を暴露もしくは公刊してはならない」。⁽⁵⁰⁾

これは電話盗聴を犯罪とした法である。同法の「なんぴと」に連邦官吏が含まれるかが問題となった。州際の酒の取引を捜査していた連邦官吏が州際の電話での盗聴を証拠として訴追した事件で、最高裁 (Roberts 判事法廷意見) は連邦官吏が含まれるとし、さらに同条に反しての盗聴による証拠は刑事事件でその能力を認めないとした。⁽⁵¹⁾ もっとも、これで連邦の盗聴による捜査がなくなったわけではない。⁽⁵²⁾

修正第四条で熱く論じられるのが、プライバシー^{トレスパス}として保護される空間はどこまでかである。⁽⁵³⁾ それはオルムステッドが述べたように、trespass (侵害) ドクトリンと関係し、刑事目的で個人の領域に踏み込むときは、犯罪捜査上相当な理由があり、令状がなければならぬとしているから、令状が要するのはどこまでかの問題でもある。最高裁は、FBI による公衆電話の盗聴が修正第四条の搜索押収に当たるとした Katz 事件^{カッツ}で、⁽⁵⁴⁾ 電話ボックス (telephone booth) が保護された空間なのかよりも、搜索押収が憲法の認める基準でなされたかを問題とした。そして、搜索押収の対象

となるのは有体物 (tangible) だけではなく、会話も含まれ、修正第四条は area (領域) だけではなくとして、政府のトレスパスを広く禁じたとした。⁽⁵⁵⁾ 原審はオルムステッドにのっとり、電話ボックスは有体財産 (tangible) ではないとした。なるほど本件では、政府の盗聴は、目的も手法も時間も限定的である。しかし、それはどのように主張しても執行権だけの判断であり、そこに司法官憲が一切介在していいとしたのである。

オルムステッドは、電話盗聴は修正第四条の搜索に当たらないと判断したもので、同条が保護するのを私人の財産の空間に限定した。カットは、囲まれた (enclosed) 電話ボックスは、家宅のように人が合理的にプライバシーを期待できる憲法上保護された場所であり、私的 (private) な場所に、物理的侵入はもちろん、電子的なそれも、修正第四条に反し、搜索令状なしに連邦政府権力が憲法上保護された領域に侵入するのには、不合理の推定が働く (presumptively unreasonable) と判断したのである。⁽⁵⁶⁾ 「修正第四条が保護するのは人であって、場所ではない (Fourth Amendment protects people, not places)」として、財物よりもプライバシーの期待の観点から、電子的監視の合憲性を判断するアプローチをとる。⁽⁵⁷⁾

最高裁はこの間、修正第四条の変化を認めている。すなわち、修正第四条は財産基盤を根源とする認識から、政府利益とプライバシーの利益を衡量して、法執行を規制するためのより一般的な道具に変容したと判断したのである。⁽⁵⁸⁾ 修正第四条が適用されるには、政府(官憲)の行為が搜索もしくは押収 (seizure) に該当しなければならない。後者は「財産上の個人の占有的利益に対する何らかの有意な干渉」と概念される。⁽⁵⁹⁾ 搜索 (search) は歴史的に憲法上保護された領域を侵害する政府のなんらかの行為を含むものであり、⁽⁶⁰⁾ この憲法上保護された領域がトレスパス理論からプライバシーへと変遷していったのである。カットでは、^(ハーラン) Harlan 判事は、搜索された対象について、当該個人がプライバシー

であると主張し、これを社会が合理的あるいは正当であると認めるにやぶさかでないとなれば、修正第四条の問題が生じるとした。⁽⁶¹⁾ 社会通念に委ねられたのであり、修正第四条が保護するプライバシー領域は、社会の発展に附随する国民の意識や公的利益で画定されるところとなる。

背景に、プライバシーの概念の成熟と国民の関心の高まり、そしてテクノロジーの進展がある。カットで Black 判事は、反対意見で次のように述べている。⁽⁶²⁾「思うに、本判決で本法廷は修正第四条の書き換えを完了させた。それはごく最近に、不合理な搜索押収に対する訴訟が個人のプライバシーと同じだとして修正第四条に不断に言及するようになったとき、始まった。…しかるに、プライバシーを保護するよう意図した本法廷の言葉に気まぐれに置き換えることで、不合理な搜索押収に対する保護を意図した憲法の文言に、本法廷は、修正第四条を、本法廷のプライバシーの最広義の概念をそこなう、憲法に反するすべての法を判示する道具にした」。もつとも、法廷意見はプライバシーを限定的に使用している。「修正第四条は、一般的な憲法上の「プライバシー権」には翻訳されえない。この修正条項はいくつかの種類の政府による侵害から個人のプライバシーを保護する。…憲法の他の規定はその他の種類の政府による侵害から個人のプライバシーを保護する。しかし、プライバシーという個人の一般的な権利―他者から放つておいてもらう個人の権利―の保護は、個々の州の立法に大きく委ねられている」。⁽⁶³⁾

カットで政府側は、本件でカバーされないケースでの例外を主張した。傍受される側の同意には、裁判所はやぶさかではないが、相当の理由の証明で司法官憲 (magistrate) が事前に授權したときは、消極となる。⁽⁶⁴⁾ もつとも、「国家安全保障を含む状況で司法官憲による事前の授權以外の防御が修正第四条を満たすかどうかは、本件で提起された問題ではない」としている。⁽⁶⁵⁾

こうした多数意見にもかかわらず、^{ホワイト}White判事は、踏み込んで、大統領や法務長官が国家安全保障の要請として電子的監視を合理的に授權したときは、令状の手続は不要だと強調している。⁽⁶⁶⁾ この指摘に押された形で、^{ダグラス}Douglas判事は、ホワイト判事の完全な青信号は疑問だとしている。⁽⁶⁷⁾ 大統領も法務長官も、司法官憲ではないし、安全保障上の事案でも中立な立場にはなく、利害当事者にほかならない。スパイや破壊者やギャングブラー（安全保障も刑事も同じということ）も修正第四条の保護を受けるのであり、刑事罰に差異はないとする。

本件で最高裁（法廷意見）は、「判事もしくは司法官による事前の承認なしに司法過程の外でなされる搜索は、それ自体（*per se*）修正第四条の下で不合理となる。特別に確立され十分に境界の画定された（*delineated*）ごくわずかな例外にのみ服する」としている。⁽⁶⁸⁾ 現実はそのような方向に展開していったとはいえない。さまざまな電子技術の発展と安全保障上の困難な脅威、特にテロリズムへの喫緊の対処の必要性が出現したからである。

カッツは、刑事司法での電子的監視には修正第四条を厳格に適用することを指示した。ただ、安全保障については別の扱いを示唆している。司法警察の手法の限界を超え、その手に負えない外国の諜報には、個人の人權と衡量したうえで、立法で限定的に電子的監視を認めるべきと指摘されるようになった。⁽⁶⁹⁾

3 Title III（タイトル・スリー）

電子的盗聴とその監視の必要性は高まり、カッツも影響して、議会は盗聴を認める規定を設けた。一九六八年、*Omnibus Crime Control and Safe Streets Act*（包括犯罪統制安全街路法）Title III（18 U.S.C. 882510-2522, ch. 119）⁽⁷⁰⁾、いわゆるタイトル・スリーに基づいて、司法警察官は、電子的監視、電話利用記録（*pen-registered*）、⁽⁷¹⁾ 交信追跡（*trap and*

trace)⁽⁷¹⁾装置、同意によるモニタリング、身体検査 (physical search)、人の監視、通報 (informants) の六つの基本的な監視の手段を獲得したのである。タイトル・スリーでは司法令状を要求しており、裁判官は「個人が、§2516で列記された特定の犯則（法定刑が死刑とされている犯罪などを列挙―筆者）を現に犯している、または犯したもしくはまさに犯そうとしていると信用するに足る相当の理由 (probable cause) が存在する」ことを発見しなければならぬ (§2518)。さらに、監視の行われる時と場所が特定されていなければならず、通常の捜査手法が尽きていることも要求される。pen-registered trap and trace には、法文上は相当の理由は要求されていないけれども、政府の法務官に進行中の捜査に不可欠だとの疎明を要求している (§2518 (a) (1))。

ここで留意すべきは、第一に、盗聴自体が厳格に制限されていることである。司法裁判官の令状が必要で、請求を受けた裁判官は相当の理由があることを判断しなければならない。カッツ判決を十分に踏まえた立法となっている。相当の理由は個別判断になるが、犯罪が行われた、あるいは行われると信ずるに足る相当な理由や事実の証明があるということである。

第二は、安全保障の捜査には適用されないとの明文の規定を置いたことである (§2511 (3))。議会は安全保障の情報収集は大統領の権限であることを気にとめ、これについてはオープンのままにしておいた。一九六八年のタイトル・スリーは、安全保障目的で大統領が外国の諜報活動を行うための電子的監視の権限には、影響を及ぼすものではないと規定した。これは、大統領には外国の諜報あるいは安全保障の目的での電子的監視を行う固有の権限があることを暗黙の前提としている。そして、次の五つの目的の行為はタイトル・スリーの射程外で、規制されないとした。⁽⁷²⁾ ①外国勢力からの現実あるいは潜在的な攻撃その他敵対行為から合衆国を防御する、②合衆国の安全に不可欠とされる外

国の諜報情報を獲得する、③外国の諜報活動から国家の安全情報を防御する、④武力その他違法な手段によって政府を転覆することに対して合衆国を防護する、⑤政府の存在あるいは構造に対するいかなる明白かつ現在の危険から合衆国を保護する。

テクノロジーの進展で、私的領域は電子空間にまで拡大していく。⁽⁷³⁾ プレモダンの修正第四条は、私人の財産の保護を意識しており、電子空間は想定していない。こうした現実にあつて、同条をアップデートさせたのは最高裁である。判例をうけて、立法が刑事司法での領域で公権力の侵害の限界を明確にさせた。タイトル・スリーはその到達点であり、刑事司法の電子的監視の実務はこれによることとなる。

4 小 括

修正第四条が適用されるためには、法執行官の行為が搜索 (search) でなければならない。それは、辞書の定義のとおりで、「本を見つげるために家を検索するとか、泥棒を発見するために森の中を探すとかのように、何かを見つげる目的で探し回る、探索する、立ち入って検証する」という意味である。⁽⁷⁴⁾ 搜索が禁じられるのでなく、それが合理的で、かつ判事の令状があれば、合憲となる。令状があれば合理的となるのではなく、国民を不安にさせる不合理な監視を行ってはならないことに主眼がある。⁽⁷⁵⁾

では安全保障の捜査の電子盗聴や監視は令状なしに行えるのか。カットは次の問題は宿題としたのである。「司法官憲による事前の授權以外の防御は、安全保障が絡む状況において修正第四条を満足させるか」。⁽⁷⁶⁾ 刑事司法に電子的監視を認めたタイトル・スリーが制定された一九六八年時点で、議会には、最高裁同様、執行権が安全保障目的で無

令状の電子的監視を行うと主張する固有の権限論を抑制する心得はなかった。⁽⁷⁷⁾

三 安全保障の電子的監視と修正第四条

1 問題の所在

修正第四条は刑事司法での手続原理を定めたものである。同条の歴史的発展の中で、法執行 (law enforcement) に電子的監視がどこまで認められるかが議論され、令状主義を厳格に確認した立法、タイトル・スリーに結実した。修正第四条はそれ以外の手続については語ってはならず、令状主義や合理性の要請が司法捜査以外にも及ぶかは、憲法上定かでない。

安全保障のための捜査 (national security investigation) に無令状で大統領が電子盗聴を命じるのは修正第四条に反さないかが初めて問題となったのが、一九七二年の合衆国対合衆国地方裁判所事件 (Keith 事件)⁽⁷⁸⁾ である。一九六八年に盗聴権限を認める立法 (タイトル・スリー) が制定され、⁽⁷⁹⁾ 特定の犯罪 (§2516 に規定される) に電子的監視 (electric surveillance) を授權している。意図的な傍受や電子的会話、電信の傍受 (intercept) は、同法に規定されたもののほかは認められないとしたうえで (§2511 (二))、法務長官に、同次官などとの内部で協議を経て、管轄権のある連邦裁判所に、FBI との会話を含む電子傍受の令状を請求する権限を認めている。ただし、安全保障上の諜報での電子盗聴には言及がない。タイトル・スリーにはどの条項も、武力もしくはその他の手段で政府を転覆させること、または政府の存在や構造にその他の急迫かつ現在の危険に対して、合衆国を保護するのに必要と考える手段をとる大統領の憲

法上の権限を制限するものと解されてはならないと規定されていた (§2511 (3))。

キース事件時、安全保障と修正第四条の情況はこうであった。⁽⁸⁰⁾一九六八年制定のタイトル・スリーで、刑事捜査のための司法警察官の電子的監視には裁判官の令状を要することとなった。これは安全保障の情報収集や諜報には適用されない。安全保障の情報収集には、FDR (F・D・ローズベルト大統領) 以降、大統領が独断でこれを決行し、トルーマン大統領が法務長官あての書簡でこれを文書化し、誰も異論をさしはさむことなく、無令状で大統領権として実行してきた歴史がある。一九五〇年代初頭、^{H・マクグレイス} Howard McGrath 法務長官はマイクロホンの監視装置を据える自らの権限を否定したが、一九五四年、^{H・ブラウネル} Herbert Brownell 法務長官はこれを覆し、長官の承認なく、FBIにかかる監視の権限が国益の許す限り認められるとのメモを出した。⁽⁸¹⁾はたしてこれが修正第四条の例外をなすのか、問題となった。⁽⁸²⁾

安全保障は大統領が広範な裁量権を有する領域であり、したがってその行動は自らの判断で秘密にしようとの伝統的な憲法観が背景にある。典型的には、ペンタゴン・ペーパー事件での ^{スチュアート} Stewart 判事の以下のような補足意見にみられる。「憲法が執行権に外交の行為と国防の維持に広範な程度の共有されない権限を与えておるなら、そのとき執行権は憲法上、その権限を成功裏に行使するのに必要な国内の安全の程度を維持し決定できる、広範には共有されない義務を持たなければならぬ」。⁽⁸³⁾この考え方は、外交に関して大統領が唯一の機関 (sole organ) であるとした ^{サザランド} Southernland 判事の考えを反映している。⁽⁸⁴⁾

憲法は国家が秘密に行動できるとする規定を設けておらない。どの機関が行えるかも規定はなく、秘密に行動できる判断の手續や審査にも言及がない。大統領に安全保障の広範な権限があり、そのために秘密に行動できるとしても、

憲法に明確な規定がない以上、そこに立法が制約的に関与してはならないとするのに説得力は見出し難く、アカウンタビリティの観点から立法的整備は可能であるとの論理も成り立つ。

安全保障には大統領の秘密指定や隠密行動の権限が憲法上認められれば、修正第四条のプライバシーの保護と対峙することになる。これが今日のNSAの電子情報大量データ収集問題の要諦といえる。安全保障とプライバシーのバランスに、技術の発達が加味される問題である。この三つともえの中で、安全保障のための電子的監視は憲法上どのように整理されなければならないのか。現代にも引きずる憲法問題として俎上にのぼることとなる。

2 Keith 判決

キースは、安全保障のための電子盗聴に修正第四条が適用されるかを判断した初のケースである。最高裁(Powell判事)は、令状主義を要求する利益と国内の脅威に対する安全保障上の利益とを衡量し、電子的監視で事前に令状を得ることを政府に要求するのは合理的であるとした。⁽⁸⁵⁾ そのうえで、ニクソン大統領の盗聴命令は違憲と判断した。⁽⁸⁶⁾

本件は、合衆国政府の財産の破壊工作に関する刑事裁判である。White Panther Party^{白パンサー党}の一味である被告の一人Plamondon^{プラモンドン}が、CIAの支局をダイナマイトで爆破した罪状に問われ、その公判で彼は政府の監視情報の証拠能力を問題として、政府が電子的監視で獲得した情報の開示を求めた。法務長官John Mitchell^{J・ミッチェル}は、政府が仕掛けていた盗聴によれば、彼がその会話に参加し政府転覆を画策していたのは明らかだとした。担当判事(Keith)は非公開(in camera)でこれを調べたが、被告側には開示しなかった。政府は、大統領には憲法上、国内の安全保障について諜報を行う固有の権限があると主張した。しかし、この連邦地裁判事キースは、われわれは法の支配に服するのであり、

人のそれではないとし、大統領が修正第四条の適用を免れるとしようとした権限には根拠がないとして、これを退けた。⁽⁸⁷⁾ 政府は急きょ、キースの命令を退けるため第六控訴裁判所に控訴したところ、原審の判断を支持したので、⁽⁸⁸⁾ 最高裁に持ち込まれた。

最高裁は電子的監視を認めるタイトル・スリーに目をやる。これは、電子盗聴を容認する状況を議会がプライバシーと衡量のうえ慎重に調整したものである。政府は、その § 2511 (3) (のちに FISA が制定され、削除されている) で、大統領が安全保障に不可欠と考える手段をとる大統領の憲法上の権限を侵害するものと解釈されてはならないとの留保規定 (いわゆる 安保書 National Security disclaimer) に依拠する。しかし、諜報に電子的監視の権限まで認めたかは、立法経緯はこの点中立であつたので、断定できない。同条が、「法文はそうした目的には全く不適切であるので、何ら権限を付与したのではないのは確かだ。本法は大統領が憲法上持ちうる権限を制限ないし邪魔立てするよう、解釈されてはならないと、規定しているにすぎない」。⁽⁸⁹⁾

ここでパウエル判事 (法廷意見) は、この § 2511 (3) が「大統領の憲法上の権限」として二つの情況の類型、すなわち、①「外国権力 (foreign power)」の攻撃、その他敵対行動あるいは諜報活動から保護する必要性がある場合、②政府の転覆あるいはその他、政府の構造や存在に対する明白かつ現在の危険から保護する必要がある場合、に言及している点に着目する。⁽⁹⁰⁾ 両方とも安全保障で語られるけれども、安全保障は外国からの脅威に関わる①でのみ使用される。②は「国内組織 (domestic organization)」から発する脅威に関わる。国内組織に明確な定義はないけれども、外国組織とは関係を持たないアメリカ人の団体組織を意味している。違法な行為の国内と外国の区別は困難で、協働している場合もある。ただし本件はこれには及ばない。外国権力の安全保障情報を収集する固有の大統領権限の射程と、適用さ

れるなら令状条項の、執行権を支配するであろう基準の問題を留保させて、国内の安全保障の脅威に本件判断を限定したのである。⁽⁹¹⁾パウエルは、国内での安全保障上の情報収集での人権侵害を懸念したのである。⁽⁹²⁾

本件は、タイトル・スリーの違憲性も、大統領の外国政府の活動に対する国内外での監視権限の範囲も、問題にしない。論点は、カツツが宿題としたように、「司法官憲による事前の授權以外の防御が、国家安全保障を含む状況で修正第四条を満足させるか」である。その鍵は修正第四条の搜索押収の「合理性 (reasonableness)」にあり、その判断は令状条項を通してなされるとする。⁽⁹³⁾ 国家の安全保障は政府の最重要の責務である。しかし、それは人権保障規定で保護される国民の自由を政府が電子的監視で侵害してよいということにはならない。カツツを含むこれまでの判例は、默示的に、電子的監視が巻き込む会話のプライバシーに政府が入り込むには修正第四条の保護が必要としている。⁽⁹⁴⁾

パウエル判事は、立法には安全保障の情報収集について規定はないと確認したうえで、大統領の安全保障権限という権力分立が問題になるとする。ただし、憲法も、タイトル・スリーも、大統領のそうした権限について触れておらない。「修正第四条は、文言上は必ずしも無制限とはしていないから、われわれの仕事は本件で問題となっている基本価値を検証し衡量することである。すなわち、国内の安全を保護する政府の義務と、個人のプライバシーや表現の自由に対する不合理な監視によって課せられる潜在的危険である」。⁽⁹⁵⁾ 修正第四条は合理的な (reasonable) 搜索であれば令状が発せられ搜索できるとしているから、裁判所は合理性を判断するよう求められている。しかし、裁判所は安全保障の観点からの合理性を判断する能力は持たない。大統領の安全保障権限も否定されるものではない。「国内の安全保障を防御する正当な必要性が政府の電子的監視の使用に必須とするなら、問題は、プライバシーと表現の自由

を市民が必要とすることが、そうした監視がなされる前に令状を要件とすることによりよく保護されうるかどうかである。われわれはまた、令状を必要とするなら、政府が自らを、政府の転覆やそれにむけた行為から防御する政府の努力をくじくことにならないかどうかとも問わなければならない⁽⁹⁶⁾。しかし、修正第四条はプライバシーを保護しており、大統領が自由な安全保障の最終的な判断者だとされる憲法上のいわれはない⁽⁹⁷⁾。本件では修正第四条での基準が求められており、「政府の監視は、その目的が刑事捜査であれ、進行中の諜報情報収集であれ、憲法で保護された言論のプライバシーを侵害する危険を伴っている。安全保障としての監視は、国内安全保障の概念がそもそも曖昧であること、諜報収集が本質的に広範かつ継続的な性質を持つこと、そして政治的反对者を監視するためにそうした監視を用いる誘惑に駆られることで、特にセンシティブである。われわれは、これまでもそうであったように、大統領に国内安全保障の役割を認めるが、それは修正第四条に適合するやり方で行使されなければならないと考える」⁽⁹⁸⁾。

なるほど令状の要請には例外はある。しかし、そうした例外は限定的で、慎重に画定される。すなわち、「一般的には、そうした例外が、証拠隠滅を防ぎ司法警察官の安寧を保護するのに警察官の正当な利益に資する」⁽⁹⁹⁾場合である。政府は、国内の安全のための例外が認められる特別の状況であり、ここに令状を事前に要するとして司法を介入させれば、大統領の権限行使を妨げると主張する⁽¹⁰⁰⁾。本件は特別の刑事訴追のための証拠収集ではなく、転覆勢力に関する諜報のための監視である。現実にはかかるターゲットを客観的に特定するのは困難で、修正第四条が要求する相応の理由は要求し得ないけれども、安全保障上の必要性は存在する。他方、公的な監視は、刑事だろうが諜報だろうが、憲法で保護されたプライバシーを侵害する恐れがある。ましてや国内の安全といった漠然とした概念では、諜報は必然的に広がり、政治的反对への監視にまで及んで、その懸念は果てしない⁽¹⁰¹⁾。

かくして政府の主張は退けられた。しかし、二つの重要な留保をしている。⁽¹⁰²⁾一つは、本件にタイトル・スリーが適用されるわけではないことである。タイトル・スリーは、「国家安全保障への国内的脅威に対応する大統領の権限を限定したり、あるいは削除したりするものではない」。もう一つは、この判断は外国の政府や機関の活動に絡むものにまで及ぶものではないということである。

では要求される令状とはどのようなものなのか。国内の安全保障の監視は犯罪捜査とは異なるとし、安全保障の令状での正当な理由には刑事とは異なる基準が適用されるとしたうえで、それは「われわれの市民の保護された権利と、諜報情報のための政府の正当な必要性の、両方に関連して正当である」かで、「令状の申請は保護に値する市民の権利の性格と執行されるべき政府利益に符合して可変的であるからだ」とした。⁽¹⁰³⁾

キース後も、ニクソンは国内の安全保障のための電子的監視をやめず、安全保障に関して外国の脅威と国内の脅威を分けるのを拒否した。⁽¹⁰⁴⁾ニクソンの電子的監視の濫用は有名であるけれども、それは付加的な犯罪行為のパターンの脈絡で暴かれたからでもあろう。⁽¹⁰⁵⁾

3 Keith 法理の課題

国内での安全保障上の捜査には修正第四条が適用されるルールをキース法理とする。海外の安全保障のための捜索はどうか。キースはその判断を留保した。しかし、その後の下級審の判決は、修正第四条の適用を刑事事件と同じようには求めている。⁽¹⁰⁶⁾Truong 事件では、「執行権の必要性は、国内の安全保障領域とは異なり、海外諜報の領域ではかくも強固なので、キースに従って統一の令状を必須とすることは、大統領の外交の責務を全うするのを不当に妨

げる (unduly frustrate)」とした⁽¹⁰⁶⁾。その理由は、第一に、安全保障として外国の脅威に対抗する試みは、最高次の迅速と秘密を要求する。これに手続の要件を課せば、諜報活動の柔軟性を妨げることになる。さらに、より重要なことに、「外交で諜報を監視するかどうかの決定をなすのに、執行権は比類なき専門性を持つているのに対し、司法権は、外国諜報監視の背後にあるデリケートで複雑な決定をなすのにはあまりにも未経験である。∴おそらく最も重要なことに、執行権は外国諜報分野で優越した専門家を擁しているだけでなく、外務に卓越した権限を有するものと憲法上企図されている」。要するに、安全保障に関する執行権の柔軟性と専門性と憲法上の権限から、裁判所は外国の諜報活動を監視するのにいちいち令状を執行権から司法権に求めさせることにはならないとした⁽¹⁰⁸⁾。

キースは、刑事捜査と安全保障の捜査は根本的に異なり、議会もこれを認識しているとした。「刑事上の監視と国内安全保障上のそれとは」別個で、「議会は後者について、(刑事上の監視)のためにすでに規定された基準とは異なる保護的な基準を考量しうる⁽¹⁰⁹⁾」。

キースを素直に読めば、安全保障の諜報活動での電子的監視は修正第四条の対象外だとはみれまい。他方、かかる活動は法執行や司法警察とは大きく異なるものしかりである。それは、目的の重大性やそれに見合った活動の秘密性や迅速性であり、令状をいちいち要求すれば、目的達成をそぎかねない。これを憲法的にどう正当化するか。

修正第四条が安全保障のための情報収集活動までは及ばないとは、裁判所は明確にしていない。キースは安全保障目的での国内の電子的監視には修正第四条が適用されるとしたのであって、それ以外は判断していない。問題は外国に対する安全保障目的での電子的監視に同条が適用されるかである。

キースの直後、下級審でこれが問題となる。一九七三年、第五控訴裁判所は、違法な銃の州際通商に電話盗聴を無

令状で行ったことについて、政府側が外国諜報を収集する目的だと主張したのをうけて、キースはこの点は白紙にしていたとし、「国内の安全保障事案では許されないにしても、外国の権力がかわつているところでは令状なしの電子的監視は合憲」とし、その根拠を憲法二条の最高司令官条項に求めた。⁽¹⁰⁾

その後も、外国政府にアメリカの国防情報の伝送を教唆した事件で、同様に、政府の盗聴は連邦通信法にも修正第四条にも違反しないとされた。⁽¹¹⁾ 修正第四条に反しないことでは、本件盗聴が「外国の諜報情報を収集する目的でのみ実行され維持されている」点を強調する。相当の理由 (probable cause) の必要性について、刑事では犯罪の存在を合理的に信じるに足ることが要件となるが、本件のように、外務に関する判断に必要な情報を得るとの重要な政府利益は重くなり、相当の理由は厳格には要求されない。大統領の最高司令官としての地位を重視する。⁽¹²⁾ 第九控訴裁判所もこの流れを踏襲し、「外国の安全保障の盗聴は一般的な令状要求に対して認められた例外である」としている。⁽¹³⁾ そうでないとした下級審判例もあるが、少数である。

安全保障の捜査として例えば、空港での無令状の荷物検査がある。これは修正第四条に違反しないのか。連邦運輸保安局 (Transportation Security Administration) は民間航空機の乗客や荷物を無令状で検査している。これについて最高裁の判断はない。ただし、税関がその職員の麻薬検査のために無令状で採尿するのは刑事捜査ではなく、不当な理由ではないから、修正第四条に反しないとした判例で、最高裁は、捜索は相当の理由に基づく令状によるのが原則とする一方、修正第四条の侵害が通常の法執行の必要性を超えて政府の特別の必要に資するところでは、具体的な状況に照らして個人のプライバシーの期待と政府利益とを衡量して判断するとし、⁽¹⁵⁾ 空港でのそうした検査は修正第四条での合理的な捜索に当たると下級審はできていると述べている。⁽¹⁶⁾ なお、特別の必要性は後に検討する。

キースはあくまで国内の電子的監視には修正第四条が適用されるとしたのであって、外国の諜報については判断していない。FDR以来の慣行も考え⁽¹¹⁷⁾ると、外国諜報のための電子的監視には同条が及ばないとも解され、現に下級審ではそう解釈している例が少なくない。この展開で、安全保障目的での電子的監視について、国内と海外とに二分されていることが鮮明にされる。国内での安全保障目的の電子的監視に修正第四条は適用されるか、されないとしてもどのような防御が考えられるか（大統領の固有権だとしてもそれは無制限ではなく、救済も含めて憲法や制定法上の制約が及ぶのか）。

安全保障の名の下に政府の電子的監視が認められるならば、修正第一条の問題も出てくる。政府への正当な反対活動や政治的その他の目的での電子交信が政府の監視のターゲットにされれば、表現の自由の問題となる。⁽¹¹⁸⁾キースはこれを意識している。いわく、「安全保障の事案は、通常の刑事事件では現れてこない修正第一条と第四条の価値の収束がしばしば映し出される。執行権の捜査義務はそうした事案ではより強い一方で、それはまた、憲法上保護された言論に、より大きな危険が存在する。歴史的には、イングランドでの言論出版の自由への闘争は搜索押収の権能の範囲の問題に絡んでいた。歴史はふんだんに、その動機がいかに思慮深くて善意であろうとも、その政策を強烈に非難する人々を疑いの目でみる政府の傾向を証明している」⁽¹¹⁹⁾。

キースは安全保障目的での連邦政府の電子的監視について、議会に手続や権限を明確にする立法制定への動機づけをもたらした。FISAである。ウォーターゲート（Watergate）事件や、CIAやNSAといった政府の秘密の諜報活動の透明化に向けた政治的な動きも、FISAの制定に影響したことは間違いない。外国の諜報だけでなく国内でも秘密裏に電子的監視が行われている懸念も、チャーチ委員会で指摘されたように、高まっていた。キースが国内の

電子的監視にはすべからく修正第四条が及ぶとした判断は、重いのである。⁽¹²⁰⁾

4 外国諜報監視法(FISA)の制定

(1) FISAの意義

アメリカの外国に対する諜報活動は建国時のワシントンの時代にまでさかのぼり、大統領が諜報機関を設置し諜報として情報収集を行ってきた。やがてFBIやCIAといった諜報機関は制定法で設置され、その活動も法の認容するところとなる。しかし、諜報活動が制定法で限界づけられることはなく、議会の監視も一九七〇年代まで存在しなかった。⁽¹²¹⁾ 議会の諜報の統制は、憲法に規定がないため、大統領の権限を侵すのではないかと、憲法問題になる。⁽¹²²⁾

キース事件の時代、つまり七〇年代前半は、ウォーターゲート事件やベトナム戦争があり、政府の諜報活動への関心が高まった。議会はチャーチ委員会を立ち上げて、CIAやFBIをはじめとする政府の諜報活動を洗い出し、その事実を把握して諜報活動に対するアカウンタビリティと統制を確保するための改革を検討した。これをうけて、諜報のための外国の電子的監視を立法で明らかにした。それが一九七八年のFISAの制定である。⁽¹²³⁾ 法務省は外国の諜報を盗聴するのに司法が制約を課すのをひたすら否定してきたが、最高裁が安全保障のための無令状の盗聴を違憲と解する余地もあつたし、ウォーターゲート事件で執行権への風当たりも強く、信頼を回復しなければならぬとのプレッシャーが立法を促した。⁽¹²⁵⁾ 議会も大統領も、外国の諜報監視の分野には制定法の授權を要し、法の支配が妥当すると認識したことになる。そこには制定法による防御や統制も盛り込まれることになる。⁽¹²⁶⁾

FISAは複雑な法であるけれども、その根本は外国諜報に関する電子的監視を遂行するのに必要な手続を規定し

たことにある。アメリカの安全保障の伝統的な手法である諜報を法的に位置付けるとともに、拡大する安全保障の諜報活動からアメリカ国民のプライバシーを保護する目的を有する。FISAの制定は、安全保障の諜報という執行権のコアを立法で規制する意義があり、そこに権力分立の問題も生じることに留意すべきであろう。

FISAは、大統領に安全保障目的での無令状の電子的監視を承認する固有の権限が認められるかの長い議論の果実である。⁽¹⁷⁾ FISA自体を違憲とする主張はさほどない。⁽¹⁸⁾ 大統領に外国の諜報のために無令状で電子的監視を行う固有の憲法上の権限があるとしても、議会にはこれを支配する合理的な令状手続を立法化することでこの権限行使を制限する権限があるとの理解が背景にある。⁽¹⁹⁾

もつとも、議会が執行権の隠密の電子的監視の統制に万全のシステムを敷いたかは議論がある。FISCI(外国諜報監視裁判所)を創設して令状主義を原則とするなど、統制の視点をメインに据えているものの、そのプロセスは不透明で、法文も執行権の利に解され、人権保障の観点から問題なしとまではいえまい。

(2) FISAの主な内容―統制の観点から

FISAは、大統領(執行権)が外国の諜報目的での電子的監視の手続を規定することで、主に以下の三点でその行使に規制をかける。第一に、令状の請求には、対象が「外国の諜報の情報(foreign intelligence information)」であって、そう判断することに相当な理由(probable cause)がなければならぬとしている(50 U.S.C. 81601(c))。外国の諜報情報とは、外国権力あるいはそのエージェントによる、(A)現実あるいは潜在的な攻撃その他重篤な敵対行為、(B)破壊工作あるいは国際テロリズム、(C)諜報サービスやネットワークの極秘の諜報活動、であって、アメリカの国防や外

交に関係するものである。(B)には二〇〇八年の改正で「大量破壊兵器の国際的拡散」が付加された。法務長官は、相
当の理由を示して、こうした外国諜報情報収集が目的であることをFISCに立証しなければならない (§1804(a)
(7))。

第二に、「電子的監視のターゲットが、外国権力か、もしくはそのエージェント」であるときのみ、令状は認めら
れる (§1804(a)(7))。外国権力とは、(1)アメリカが承認しているかどうかにかかわらず、外国の政府もしくはその部
分、(2)実質的にアメリカ人で構成されていない外国の分派、(3)外国政府が公に認知している実体で、そうした政府が
指揮統制している、(4)国際テロリズムあるいはその準備活動に従事している集団、(5)実質的にアメリカ人で構成され
ていない外国に基盤をおく政治組織、(6)外国政府が指揮統制する実体、である (§1801(a))。外国権力のエージェン
トとは、非アメリカ市民であつて、(A)上記の(4)で定義された外国権力のメンバーとして、もしくは外国権力の官吏ま
たは被傭者として、アメリカで活動しており、(B)アメリカの利害に反して、アメリカ国内で極秘の諜報活動に外国権
力のために従事しており、そうした者がアメリカにすることがそうした活動に従事していることを示している、もし
くはそうした者が故意にそうした活動を支援している、または教唆しているとき、と定義される (§1801(b)(1))⁽¹³⁾。

FISAが認める捜査手法には、(1)電子的監視 (50 U.S.C. §1803(a))、(2)身体検査 (§1822(c))、(3) pen register
and trap (電話利用状況記録) (§1842(a)(1))、(4)有体物 (tangible things) 作成強制命令の使用 (§1861(b)(1)) がある。
二〇〇八年のFISA改正法で、外国にいと合理的に信じられている非アメリカ人やアメリカ人をターゲットにする
外国諜報も認められるようになる⁽¹³⁾。

第三に、許される電子的監視の手法は、以下のように限定している (§1801(4))。すなわち、(1)アメリカ国内にい

る特定のアメリカ人向けられた、あるいは受信された有線無線通信を含む有線無線通信監視装置を含む電氣的、機械的、その他監視装置による取得で、内容が、意図的に当該アメリカ人をターゲットにすることによって取得され、人が合理的なプライバシーの期待をもち、法執行のためには令状が必要とされる状況下にある場合、(2)アメリカ国内にいる人へ、もしくはアメリカ国内から、有線無線通信を含む有線無線通信監視装置を含む電氣的、機械的、その他監視装置による取得で、アメリカ国内で行われ、いかなる当事者の同意も得ていない場合、(3)アメリカ国内にいる特定のアメリカ人向けられた、もしくは受信された、有線無線通信を含む有線無線通信監視装置を含む電氣的、機械的、その他の監視装置による意図的な取得で、内容が意図的に当該アメリカ人をターゲットにすることによって取得され、人が合理的なプライバシーの期待をもち、法執行のためには令状が必要とされる状況下にあり、送信者も意図されたすべての受信者も合衆国内にいる場合、(4)アメリカ国内で情報を得る監視のための、有線無線通信以外からの電氣的、機械的、その他監視装置の使用あるいは設置で、人が合理的なプライバシーの期待をもち、法執行のためには令状が必要とされる状況下にある場合、である。この定義で法執行、つまり刑事司法のための証拠収集たる監視では別の令状を要すること、法執行と諜報の間に「壁」を作っている点に留意したい。

FISAは安全保障目的の電子的監視において、諜報機関に二つの手段を認めた。第一に、法務長官は、当該監視が「外国権力」間でのみの通信に向けられ、「アメリカ市民」の通信を取得する意図がなく、その可能性がないと確信したとき、一年以内の監視を授權することができる。⁽¹³²⁾ 第二に、それ以外の電子的監視で、法務長官が電子的監視あるいは物理的搜索の対象となる施設や財産が外国権力のためにのみ使用され、アメリカ市民の通信を取得する実質的可能性がない法定の情報であるとの確証を提示して、FISCに申請し、その命令を以て行う電子的監視である。⁽¹³³⁾

後者の手続が原則で、前者は例外的である。⁽¹³⁴⁾ FISCtの令状が原則として必要だということである。

FISCtへの申請は、FBIまたはNSAのエージェントが署名した宣誓供述書 (affidavit) の入った法務省司法官 (magistrate) 署名の申請書と、FBI長官のような最高幹部の署名した確証書の二点を要する。⁽¹³⁵⁾ これらで、電子的監視の対象となるターゲットの特定と、それが外国権力あるいはそのエージェントであるとの相当の理由を確証させなければならない。ただ、これはタイトル・スリーが同じ「相当の理由」とするも、それが、当該個人が特定の犯罪を犯している、あるいは犯したと信じるに足るのに相当である理由であり、その特定の犯罪に特定の交信が取得され、それが関連していると信じるに足る相当な理由としている点で (18 U.S.C. § 2518)、FISAの方は緩やかといえる。また、タイトル・スリーは交信を特定させて限定しているのに対し、FISAは、外国からの攻撃あるいはテロ、秘密裏の諜報活動からアメリカを守るのに必要な「外国諜報情報 (foreign intelligence information)」と広く括っている (50 U.S.C. § 1801 (e))。

概して、タイトル・スリーに比べれば、FISAは政府側に緩やかな規制となっている。電信傍受の期間では、タイトル・スリーは三〇日間に限定し、延長は裁判官によってさらに三〇日間を限度として認められる (18 U.S.C. § 2518)。また、傍受 (interception) 終了から九〇日以内に傍受された者にその情報が提供される。FISAは傍受の期間を九〇日から一二〇日とし、一年間まで認められることもある (50 U.S.C. § 1805 (e))。傍受の名宛人に通知することは要求されていない。またFISAでは、ターゲットが同定されていなくても電子的監視は認められ (50 U.S.C. § 1804 (a) (3))、法務長官に緊急命令を認めている (§ 1805)。電子的監視ではタイトル・スリーよりFISAの方が執行権にとってハードルが低い⁽¹³⁶⁾ため、連邦レビューではその八五%がFISAによるといわれる。

FISAの法文上は、警察機関が外国の諜報目的での情報と区別するための明確な線引きはなかったけれども、制定時は電子的監視はともかく、防諜での使用を認めていなかった。執行権は、blackbag jobs（諜報の情報入手のための不法侵入）といわれる物理的な搜索は固有の権限であると解していた。しかし、一九八一年にFISCIが立法にこれを授權する規定がないと判示したので、FISAを改正して身体検査を認めた⁽¹³⁷⁾。それは、「合衆国内で、情報、資料、あるいは財物の押収、再生、探知、あるいは変更を惹起するのを意図した不動産あるいは財物（技術的な意味での屋内の財物の検証を含む）への物理的な侵害（physical invasion）であつて、人が合理的なブライバシーの期待をもち、法執行目的では令状が要求される状況にある場合」である。ただし、FISAの定義する電子的監視や他の法による合衆国政府の外国諜報情報の取得を含まない。

FISAで政府がビジネス記録の提出を強制できるのは、もともと、外国の諜報もしくは国際テロの捜査に必要とされる四つのタイプの事業者、すなわち、一般通信事業者（common carriers）、公共施設（public accommodation facilities）、倉庫（storage facilities）、自動車レンタル（vehicle rental facilities）であつた。これが愛国者法（USAPATRIOT Act）二一五条によつて対象が広がられて「知覚できるもの（any tangible thing）」とわれ、二〇〇五年の同法のさらなる改正では、求められた知覚できるものが授權された捜査に関連する（relevant）と信じるに合理的な理由があることをFBIが示せばよいとした⁽¹³⁸⁾。「合理的」とか「関連性」とかには明確な定義がないけれども、相当な理由（probable cause）よりも緩やか要件である。

FISAは、アメリカ国内で外国政府あるいはその機関と交信していると疑われる外国人の電子的監視を認めた。合衆国外での交信は完全に除外されている。それがアメリカ人への最小限化手続（minimization procedures）を満た

し、⁽¹³⁹⁾ かつ監視の目的が外国の諜報情報の獲得であり、他の捜査手法では合理的に獲得できない情報であるのが明らかに誤りでなければ認められる。⁽¹⁴⁰⁾ 令状を求める司法長官は、外国の諜報情報を流布させ取得し加工する必要に応じて、同意を得ていないアメリカ人に関する公情報の取得と留保を最小限にし、流布を禁じる特定の監視の技術と目的に照らして、合理的に企図された特別の手段 (special procedures) を策定するものとしている。ここでは、アメリカ市民が同定されて流布されることがないように配慮している。

(3) 電子的監視の司法的統制

諜報活動の統制のために、これを許可する司法的機関として FISCt を置いた。⁽¹⁴¹⁾ 制定当初、最高裁長官によって任じられる七人の司法判事で構成されたが、二〇〇一年のいわゆる愛国者法で一人に増員され、うち三人はワシントン DC から二〇マイル以内に居住することとされた。任期は七年である。FISCt の控訴裁判所 (Foreign Intelligence Surveillance Court of Review (FISCR)) も置かれ、最高裁長官が任じる三人の判事で構成される。⁽¹⁴²⁾ FISCt は、NSA や FBI の請求をほぼ認めるゴム印と化しているともいわれており、また、審理は秘密で政府関係者のみが当事者であることから、統制の実という点では疑問もあろう。⁽¹⁴³⁾ FISCt の改革が議論されている。⁽¹⁴⁴⁾

一九七九年以来これまで (二〇一三年) に、約三四〇〇〇の外国諜報監視のための国内の電子的監視、物理的搜索、両者の結合についての令状申請が、FISCt になされている。⁽¹⁴⁵⁾ その詳細は議会に報告することが、立法で義務づけられている。カーター大統領期で五一八件、レーガン大統領期で四二九四件、ブッシュ大統領 (息子の方はブッシュ 43 と記す) 期で二二一八件で、この間には一件の否認もない。クリントン大統領には一件の否認を含む六〇五七件、

ブッシュ43大統領では一四三三三件（九件の否認）、オバマ大統領（二〇一二年まで）では六五五六件（二件の否認）である。FISA制定から三年間は約一四〇〇〇件で年平均六〇〇件であったのが、九・一一以降、年平均が約三倍の一七〇〇件に増加している。

制定当初、司法裁判所はFISAの電子的監視を厳格に解し、その「主たる目的（primary purpose）」が外国諜報情報の獲得ではなく刑事訴追であるならば、認められないとした。⁽¹⁶⁾ 電子的監視には、刑事司法と安全保障の諜報の壁が厳格に意識された。しかし、九・一一後の愛国者法によってFISAが改正され、「その目的（the purpose）」ではなく「相対的な目的（significant purpose）」が外国諜報情報の獲得にあれば、電子的監視が認められるとされた。⁽¹⁷⁾ また、FBIはFISAの監視をするときには、FBIの刑事部（Criminal Division）に相談することが認められた。⁽¹⁸⁾ ただ、FISAの対象となる諜報情報はスパイや組織犯罪など、刑事事犯とも密接に関連していることが少なくない。⁽¹⁹⁾

このFISA改正は修正第四条に違反しないと判断されている（In re Sealed Case）。⁽²⁰⁾ FISA上の命令は中立の分離された司法官憲（neutral and detached magistrate）によるものだから令状に類し、監視の期間や対象とされる情報も限定されている。⁽²¹⁾ FISAに基づく監視は合理的であり、テロリストやスパイの脅威から国家を保護するという、法執行の通常の必要性を凌駕する政府の「特別の必要（special needs）」の利益と個人のプライバシーの利益は適切に衡量されているとした。⁽²²⁾

In re Sealed Caseでは、愛国者法によるFISAの改正が是認された。本件は、FISCTが監視命令に条件を付けたことで政府がその控訴裁判所たるFISCRに控訴した初めてのケースである。刑事司法と外国諜報の監視の間に壁が設けられたが、FISCRは、一九七八年制定時のFISAには、政府の集める諜報情報は刑事訴追に一切

使用されないとする排除の意図はないと解釈した。⁽¹⁵³⁾

最高裁は、修正第四条の安全保障情報の収集への射程は明確にしていない。現実には、安全保障の情報収集や諜報は同条の蚊帳の外でなされるようになる。これにルールを設けたのがFISAであり、以後諜報は同法で論じられるお膳だてがなされたこととなる。しかし、FISAが規定しない国内の諜報については、法的問題が残った。

議会制定法であるFISAにより、安全保障上の捜査に執行権の権限と手続が明確にされたけれども、依然として、外国の諜報監視における大統領の憲法上の専権性との緊張関係は続く。条文と運用と制憲者意思、そして判例（司法権は、修正第四条は安全保障上の外国の諜報監視には適用されないとしている）から、大統領の固有の諜報権限が認められ、FISAはだまし（fraud）で違憲だとの主張もある。⁽¹⁵⁴⁾

こうした司法的な統制に加えて議会による監視も制度化している（50 U.S.C. § 1881d）。最低でも半年に一回は、法務長官は両院の安全保障諜報司法委員会のルールや議会規則に従って、FISAの執行に関して同委員会に十分に報告しなければならない（a項）。その中身は § 1881a、§ 1881b、§ 1881c の各条に関する事項と法定されている（b項）。

（４） 刑事司法捜査と安全保障上の捜査との「壁」

FISAは無令状を含む、外国の諜報のための電子的監視を認めたものであるから、修正第四条の関心から重要なのは、それが法執行、つまり刑事司法捜査とは厳格に一線を画さなければならないということである。これは壁と呼ばれ、FISA以前から存在していたともいえる。⁽¹⁵⁵⁾ 最高裁は、証拠とするために無令状で私的書簡などを押収したことは、修正第四条に反するとして本人に返還する義務があるとし、同条違反の証拠能力を否定している。⁽¹⁵⁶⁾ 同条は違反

の効果は規定していないけれども、裁判所は排除法則 (exclusionary rule) を読み込んでゐる。判例は刑事捜査と安全保障目的の情報収集を区別しており、後者は前者ほど厳格な手続を要しないとしている。

FISAは、電子的監視にはその「主要目的 (primary purpose)」が諜報であることを要件とした(後に愛国者法により「相当な目的」に緩和)。これはトゥルーションが確認しているように、⁽¹⁵⁷⁾ 刑事と安全保障の捜査を厳格に区別し、刑事が主要な目的となれば令状が不可欠になるとの法理を示したものである。法執行機関を持たないCIAと異なり、FBIは安全保障の諜報と法執行の司法警察権の両方を有する機関である。内部では部署は分かれているものの、安全保障の諜報対象は刑事事犯になることも多く、相互で情報交換等を行えば安全保障上の危険事犯を防ぐことになる。FISAの対象となる外国権力のエージェント等が同時にテロ犯罪などの刑事事犯の容疑者である場合もありえよう。FISAは、安全保障目的の捜査手法は刑事司法のそれに使用されてはならないことを明らかにし、FBIあるいは法務省ではFISAの壁と称して、法執行と安全保障捜査部門との情報や意見の交換が制限される⁽¹⁵⁸⁾としてきた。

一九九五年七月一九日、時の法務長官 Janet Reno の出したメモ「外国諜報及び外国防諜の捜査に関するFBIと刑事部のコンタクトの手続」(Wall Memo)は、法務省内の刑事司法と諜報や防諜の職務が適切に調整されるのを図ることを目的とする⁽¹⁵⁹⁾。ただ、このメモでも交流を断絶させるのではなく、むしろ適切な調整、つまりルールをはっきりさせることを主眼としている。外国の諜報や防諜にFBIの部局が電子的監視や身体検査を行うとき、それが事実や状況からして重要な連邦犯罪が犯されたと合理的に判断できるならば、FBIと諜報政策審査局 (Office of Intelligence and Policy Review (OIPR)) は刑事部 (Criminal Division) に知らせ、刑事部がFBIと実質的に相談する前にOIPRに通知する。FBIは、OIPRと刑事部の承認がなければ、そうした捜査には法務長官官房とコンタクトしてはな

らない。法務省はトゥルーオンの主要目的テストを核としており、これがFISAの壁の根源である。⁽¹⁰⁰⁾

壁は、⁽¹⁰¹⁾九・一一をうけて制定された愛国者法前後で変容する。法務省は九・一一後まもなく、諜報と法執行のより大きな調整を可能にするFISAの改正を議会に提案しており、それで「主要目的」が「相当な目的 (significant purpose)」に改正された(愛国者法二一八条)。二〇〇二年には法務長官 Ashcroft は、外国の脅威から安全を保障する必要性は、「十分かつ自由な交換」をやむを得ないものにしていて、諜報と法執行の間での完全な情報と助言の交換を可能にする手続を示して、Wall Memo によって代わっている。

さらに愛国者法は、電子的監視および身体検査では、FISA 令状を執行する連邦官吏は、外国権力もしくはそのエージェントの、(1) 現実あるいは潜在的な攻撃またはその他の重篤な敵対行為、(2) 破壊行為または国際テロリズム、(3) 秘密裏の諜報活動やそのネットワーク、の捜査あるいは防衛のために、連邦法執行官吏と相談できるとした。⁽¹⁰²⁾

二〇〇二年の In re Sealed Case Ⅱ FISC R は、そうした調整が法執行に捜査の裁量を認めこれを統制することになるとしても、FISA は法執行と諜報の間の完全な調整を意図しているとして、この二〇〇二年の手続を認めている。⁽¹⁰³⁾ただし、「相当な目的」の制約がかかり、それは法執行でない相当な目的がある限り、FISA はテロ事犯にも主要なものとして使用されうることである。⁽¹⁰⁴⁾かくして、FISA でも刑事訴追の証拠収集が限定的に認められることとなるが、そうした刑事事犯は限定されている。すなわち、刑事事犯には「外国諜報犯罪 (foreign intelligence crime)」と「通常犯罪 (ordinary crime)」の二つのカテゴリーがあり、前者について可能というのである。⁽¹⁰⁵⁾

壁はFISAに基づく監視を包括的に制限するものではなく、法執行、司法警察権との内部組織的調整を要すると

いうことである。⁽¹⁶⁶⁾ FISAによる捜査の対象や方法が特段、壁によって変わるわけではなく、壁のあることでプライバシーなど人権保障に資するという⁽¹⁶⁷⁾ことでもない。壁が憲法上要請されるかといった次元までさかのぼった議論はさほどなされていないようであり、壁の是非は立法政策上の問題といえよう。⁽¹⁶⁸⁾ ただ、タイトル・スリーとFISAの両方が選択可能であるとき、イージーなFISAの令状に訴えることが多くなり、人権保障の観点から問題とされる。⁽¹⁶⁹⁾

現行のFISAは、他の機関や連邦官吏がFISAに基づいて収集された情報を名宛人に通知することなく使用するのを認めている (§1806(a))。ただし、minimization procedure (最小限化手続) に適合している限りである。FISAで収集された情報は、あらかじめ法務長官が刑事訴追目的での使用を許可しておらず、そうしたことが宣言されていない限り、法執行目的での開示はされない (§1801(b))。

もっとも、連邦の職員は、安全保障目的で収集された情報を、特段の法律の規定がなければ、自らの公務の執行に必要な限りで、そうした情報を無許可で開示するのを制約される条件で使用できる (50 USC §4355d)。愛国者法で追加された §1806(k) は、外国の諜報の情報を得るために電子的監視を行う連邦官吏は、法執行官吏に相談することができるとし、電子的監視について法執行と諜報の壁はさりげなく取り払われたようにもみえる。

四 安全保障捜査の電子的監視のコンプレックス—修正第四条の守備範囲と権力分立

1 プライバシー—空間の限定

最高裁は、警察が pen-register and trap (誰に電話を掛けたかの記録) や通話記録 (誰から電話を受けたか) を使って

獲得した証拠は、憲法上保護されたプライバシーを含むものではないと判断した (*Smith* 判決)⁽¹⁷⁾。ボルチモア警察は窃盗犯の捜査に無令状で電話会社を設置させた *pen-register* で、被告人の通話記録を収集していた。これが修正第四条に反さないかが、問題となった。電話の契約者は電話会社に自分のとダイヤルした番号を伝えており、そうした電話番号にプライバシーの主観的な期待は存しないのであって、自発的に第三者に引き渡した情報に正当なプライバシーの期待 (*legitimate expectation of privacy*) などもないとしたのである⁽¹⁷⁾。*pen-register* は電話の会話の本身ではなく、電話番号の記録の装置に止まり、番号自体は自発的に契約者が電話会社に伝送したものであって、そこで電話会社の保有する情報となる。この解釈、すなわち個人は第三者と情報を共有する場合、もしくは第三者との取引ないし交信の一部として情報が流通する場では、プライバシーの保護を失うとするルールは、第三者の法理 (*third-party doctrine*) という判例法理を形成している⁽¹⁷⁾。

電話番号等をプライバシーとして保護するために、電信記録追跡装置法 (*Pen Register and Trap and Trace Devices Statutes*) を議会は制定している⁽¹⁸⁾。電話番号は憲法上は保護されないことを前提としたうえで、これを立法で保護した。一九七四年にプライバシー法を制定し、自己に関する政府のコンピュータ情報の確認や訂正の権利を認めている。

社会が合理的と認識しているプライバシーの期待を本人が持ったかどうかのカットのテストは、踏襲される。最高裁は、マリファナを自宅で栽培しているとして、被告人宅にサーモスタット (温度が上がっているのはマリファナを栽培している証拠となる) を無令状で仕掛けたことが、修正第四条に反するとした (*Kyllo* 事件)⁽¹⁹⁾。家の中の熱の相対量をはかるために公道から私人宅に向けたサーモスタットは、同条の搜索 (*search*) に当たるとしたのである。カットのテストには、法廷意見を書いた *Scalia* 判事も主観的に予見できるものではないと批判的であったが、コモンロー上ブラ

イバシーには最低限の期待はあって、何が合理的かにも合意があり、それは家の中やカバーのかけられた家具や自動車や電話ボックスなどがそうで、本件はまさにこれに当てはまるとした。⁽¹⁷⁶⁾

もともと、家の外部にサーモスタットを取り付けて温度の上昇を観察するのは、コモンローではトレスパスには当たらないし、また会話を聞くわけでもないの、プライバシー侵害になるかは微妙である。また、家の温度は常識的にプライバシーと認識できるものなのかも知れぬ。政府が主張するように、家から出る熱だけを観取するのだから、盗聴のようにむき出しの、まさに無許可で私宅に土足で入るのとはわけがちがう。反対意見⁽¹⁷⁷⁾ (O'Learyの判事)は off the wall (壁から離れている) と through the wall (壁を通して) の区別の憲法的意義を強調する。後者では私的空間に観察者は直接アクセスできるが、そこからいかなる考えを導き出すかは公的空間とみる。本件は off the wall であり、観察者は家の外にあるのである。多数意見はこれを取らず、いわばリパリアン的に、修正第四条は「家の入口に強固な線」を引いたのだとする。

最高裁は、一〇日間と許可した令状で、一日目に麻薬売人の容疑者の車にGPS (Global Positioning System) を二八日間取り付けたのは、修正第四条に違反すると判示している (Jones 事件)⁽¹⁷⁷⁾。政府が明白に情報を得るために物理的に個人の財産を占有しており、したがって物理的侵害があるから、同条の搜索に当たるとしたのである。⁽¹⁷⁸⁾

オルムステッドを思い出してみよう。修正第四条が保護した私人の空間は、古典的にはトレスパス法理での、物理的に本人の手の届く範囲の有体物であった。これだと電子空間は保護されない。ブランドイスの反対意見は、修正第四条は技術の進歩と歩調をあわせなければならないとしていた。⁽¹⁷⁹⁾ その後電話盗聴をめぐる、合理的にプライバシーが期待できる空間だとして、修正第四条の保護を認めた (カッツ)。ハーラン判事の提示した合理的プライバシー期待

テストは同条の保護領域の判断基準となり、カイロでも新技術に対応した判断が下された。⁽¹⁸⁰⁾

法廷意見を述べたスカリアは、「修正第四条の判例はコモローのトレスパスに結び付けられていた」としたうえで、サーモスタットの装置は家の外の公用財産に据えられていたけれども、家の中の様々な熱を暴露するもので、熱から帰納される情報を取得することになるから、修正第四条の搜索（search）に当たるとした。⁽¹⁸¹⁾「家の内部の搜索の場合―典型的ゆえに保護されたプライバシーの領域であると、最も訴訟にされる―コモローに深く根差して、存在するプライバシー最低限の期待であり、ゆえに合理的と認識されているあらかじめの基準（ready criterion）がある。この最小限の期待の保護を取っ払えば、修正第四条によって保障されたプライバシーを警察の技術で侵すのを許すことになる。感覚向上の（sense enhancing）技術によって、その他の手段では憲法上保護された領域に物理的に侵入（physical intrusion）せずには獲得されえない屋内の情報をなんでも獲得することは、搜索に当たる―少なくとも（本件のように）問題となっている技術が一般的には公用に至っていないところでは」。⁽¹⁸²⁾ ジョーンズはやはり新技術たるGPSが問題となったが、合理的プライバシーのテストは取らず、古典的な財産法のトレスパスのテストで判断している。ただ、カットで示された合理的プライバシーのテストはコモロー上のトレスパスのテストにとって替わるのではなく、付加されるものであるとしている。⁽¹⁸³⁾

プライバシーの射程は一義ではない。この不確実性（uncertainty）はテクノロジーの急速な変化によってもたらされた。最高裁判事 Breyer は、それは、プライバシーに対するわれわれの関心によって価値が複雑多様化していること、新技術に適応すべき新たな法制度の必要性がすでに複雑であること、こうした複雑さに法領域が競合する（時に対立する）関心のバランスを取るのは困難であること、の三要因があると整理している。⁽¹⁸⁴⁾

問題は、修正第四条は何を保護しようとしたのか、保護された権利は何か、である。判例では、個人の財産とする古典的流れがある。これにプライバシーを加えるのが判例とみるか、ここでは修正第四条は保護していないと読むかの争いがある。ブランドイスのようにプライバシーまで保護したとみるのが多数のようであるが、最高裁は必ずしも明確ではないようだ。保護された権利の画定が同条の意義を決定するといえる。

同条は権利として「保全される権利 (right to be secure)」を置いている。これが何かを探るのが肝要であろう。⁽¹⁸⁶⁾ オルムステッドは物理的にとらえるも、その後カットで、プライバシー、つまり物理的に限定されず、私的な空間の聖域化が図られる。カットはトレスパス理論からシフトさせて、修正第四条はプライバシーを保護したと判断した。これはオルムステッドの判例を変更したと読むのが自然であろう。一方で、むしろ古典的財産観念を踏襲しているとの見方もある。ただ、プライバシーの合理的な期待の具体的な範囲や中身を判例は明確にしておらず、実際にどこまで保護されるかは不明瞭なところもある。⁽¹⁸⁶⁾

カットが、修正第四条で保護される空間をオルムステッドのように目に見える物権的対象には限定されなかったのは明らかだ。「修正第四条が人であつて単なる領域ではないものを不当な搜索押収から保護すると認識された以上、同条の射程が何らかの与えられた囲い地への物理的な侵入があつたかどうかにとどまらないことは明確になる」。⁽¹⁸⁷⁾

修正第四条の保護領域の画定は、テクノロジーの発展に伴い、犯罪やテロの手法の複雑さとそれらを捕捉する権力側の高度な技術の必要性のあえぎの中で、プライバシーの概念を精緻にさせるとともに、公益（安全保障）と私益（プライバシー）の調整が憲法問題として先鋭化してくることとなる。また、修正第四条の令状主義は政府がプライバシーに介入する場合のすべてに要求されるわけではなく、制憲者も例外があると認識している。令状主義が認められない

場合はあるのか、それはいかに正当化されるかの議論が重要となってくる。

2 特別の必要性の法理

政府がEメールなどサイバー空間に出た情報を収集分析しても、修正第四条の問題は発生しないとする解釈に、特別の必要性 (special needs doctrine) の法理がある⁽¹⁸⁾。Eメールは誰が誰に発信したかは、プロバイダーなど第三者の手を介していることから、その時点でもはやプライバシーを論じる意味がなく、そこを政府が監視しても修正第四条の問題は生じないとの考えがある。これを発展させて、通常の法執行活動を超える目的で、令状を要すればその目的達成を阻害することとなる場合は、修正第四条の射程外とする理論で、判例で認められている。裁判所は公的、私的さまざまな利益を衡量しながら状況を斟酌して、個別に判断していくことになる。

海上運輸安全法 (Marine Transportation Security Act) に基づくチャップラン湖のフェリーでの手荷物や車両の検査がプライバシーの侵害だと訴えた事件で、⁽¹⁹⁾最高裁は政府の利益が勝ると判断した。その際、裁判所は以下の三点に着目した。第一に、政府の侵害の性質や程度である。検査は短いもので事前に告知しており、プライバシー侵害を最小限にするように配慮されているとした。第二に、そうすることの差し迫った必要性の性質である。大規模なテロ攻撃を未然に防ぐ利益を認め、麻薬検査は空港などで実際に行われており、政府は特別の必要性を立証する責めを負わな⁽²⁰⁾いと⁽²¹⁾した。第三に、そうした必要性を示す政策の効率性であり、テロ予防に合理的関連性があると認めた。そして特別の必要性には、ターゲットを特定しておくことは要求されない。テロ攻撃の高度の危険性の判断では、裁判所は沿岸警備隊 (Coast Guard) の決定に委譲するとした。

二〇〇八年のFISA改正によって、DNIと法務長官がアメリカ国外にいると合理的に推測できるものに電子的監視を認めた規定が修正第四条との関係で問題となった。⁽¹⁹⁰⁾ アメリカ保護法 (Protect America Act, Pub. L. 110-55, 110th Cong. Aug. 5, 2007) に基づいて、電信プロバイダーにその一定の顧客を無令状で監視するよう命じることが修正第四条に反しないかが、論じられた。同法は、アメリカ国外にいると合理的に信じられる標的に、令状なしの外国諜報の監視を認めている。監視が外国諜報のプログラムに基づいており、外国人には同条による保護は及ばず、また安全保障であって法執行活動ではないから、情報収集の喫緊性も高いとした。⁽¹⁹¹⁾ 政府の利益は「最高次の秩序 (highest order)」であり、正当な私的利益を適切に保護する「防御の母体 (matrix of safeguard)」があるとした。⁽¹⁹²⁾

これは、刑事司法を超える国家利益には修正第四条の令状主義が適用されないとする法理である。最高裁もこれを認めている。⁽¹⁹³⁾ 法執行の通常の必要性を超える特別の必要があり、なおかつ疑わしいとの理由があれば、無令状で捜索できる。国境の防御などがこれに該当する。麻薬取引を捕まえるための高速道路での検問は、政府の主要目的が通常の刑事犯の証拠を単に発見することにあるから、特別の必要は認められない。⁽¹⁹⁴⁾ なるほど麻薬売人を捕らえるのは困難であるけれども、目的は主観的ではなく実務的に判断される。メキシコ国境から一〇〇マイル内に検問所を置くのと、飲酒運転者を拘束するための検問とでは、後者は高速道路での飲酒運転による危険を避ける目的であり、法執行目的と変わらないとしている。テロは刑事犯だとしても緊急性が認められれば、それは脅威と同義とで、通常の刑事司法の枠を超えたとする。

特別の必要性の法理は、修正第四条が適用されるかの判断で、プライバシーと政府利益を衡量するけれども、その限界は明確ではない。「われわれ市民の保全とプライバシーを保護する修正第四条の目的を弱める危険な兆候」との

述懐もある。⁽¹⁹⁶⁾ ニューヨークの地下鉄の搜索プログラムが対テロの必要性和目的から同条に違反しないとされたケースは、地下鉄という、プライバシーがすでに減じられた空間であるとの認識をベースにして、政府利益を重んじるとともに、プライバシー利益との衡量を同法理の分析で軽量化する傾向を示したとされる。⁽¹⁹⁷⁾

特別の必要性は法であるけれども、野放しにしておいてよいわけではない。これは憲法というより立法政策の問題かもしれない。サイバー空間を政府が監視するときは、独立した機関による事前の審査と同意が原則必要とされねばなるまい。立法でFISCtの許可を必要とさせる途もあろう。⁽¹⁹⁸⁾

3 権力分立と修正第四条

(1) 安全保障と大統領

二〇世紀以前は、安全保障情報の収集は戦時に限られていた。⁽¹⁹⁹⁾ 制憲者は、すべての搜索押収に修正第四条が適用されて令状を要すると考えてはいなかったようだ。⁽²⁰⁰⁾ 安全保障の権限は大統領にあると考え、それに不可欠の情報収集の権限も有するとしていた。議会は秘密を守るにはあまりにも人が多すぎるので信用ならないが、独任の大統領は秘密を守れるというのである。⁽²⁰¹⁾ 実際、FDR以来、大統領は令状なしで安全保障の電子的監視を行ってきた。⁽²⁰²⁾

諜報活動、つまり安全保障のための捜査は憲法に規定がないので、大統領に固有の権限なのか、それとも立法によって権限が確定される、つまり議会の権限なのかは、権力分立の憲法問題になる。Youngstown事件^{ヤングスタウン}でのJackson^{ジャクソン}判事の三類型テストによれば、⁽²⁰³⁾ 憲法上権限の所在が明確でない場合、^{曖昧領域} twilight zone となり、議会の立法がこれを確定させることになる(第二類型)。しかし、大統領に憲法上の安全保障権限があるので、諜報は第三類型と解され、大統領

領が固有の権限に基づいて、つまり立法の制約を超えて十全な裁量が認められる。実務では支配的な「排他的大統領 (presidential exclusivity)」であり、その根拠を制憲後の歴史 (post-ratification history) に求め、F D R 以来の大統領の専権としての諜報活動とこれへの議会の忍従 (acquiescence) をことさらに強調する⁽²⁰⁴⁾。

最高裁は総じて、安全保障には大統領に広範な権限を認め、憲法は諜報 (intelligence) をどこにも規定していないが、大統領の憲法上の地位にその根拠を認めている。いわく、⁽²⁰⁵⁾「大統領は、最高司令官と外交上の国家機関の両方として、報告が世界に公開されていない、そしてされるべきではない諜報活動を利用することができる。裁判所が、関連する情報なしに、適切に秘密と判断された情報をとりあげた執行府の行為を審査したり、無効にしたりするようなことは、許されまい (would be intolerable)」。

ここで問題となるのは政府、とりわけF B IやN S A、C I Aといった政府諜報機関が、安全保障の情報収集の際、令状なく盗聴のために電子的装置を取り付けて活動できるのか、言い換えれば、司法裁判所の許可なくそうすることが修正第四条に反しないか、である。その焦点は令状が要求されるか (warrant clause) なのである。これは刑事司法手続ではなく執行権の権限行使のための情報収集であるから、行政手続といえようか。

憲法の適正手続原理は行政手続にも適用される⁽²⁰⁶⁾か。もとより、修正第四条は刑事手続に適用されることを意図している。安全保障のための家宅侵入などは、同条は想定していない。さらに、安全保障の情報収集は憲法二条で認められた大統領権限であるとして、修正第四条をストレートに当てはめるのを懸念する憲法思想がある。そもそも修正第四条は、令状主義などの手続は規定せず、それを立法に委ねたと解され、議会によって同条は具体化される。その際、安全保障の情報収集まで令状主義を要求したとすれば、大統領の権限を侵害すると論じられる。修正第四条は安全保

障捜査にも何らかの役割は果たすであろうが、ごくごく控えめなのである。⁽²⁰⁷⁾

ケッ
Leit は司法裁判官が安全保障の領域に入ること自体、その能力を超えているのを否定できないとする。⁽²⁰⁸⁾ まず、そうした安全保障のための令状には現行法上どのようなものがあり、どのように機能するのかは、オープンのままである。⁽²⁰⁹⁾ 裁判所は、政治部門がそうした令状主義を裁判官によってどのように機能させようとしているのかは、はかりえない。さらに、監視の技術に不案内だし、外交的取極でどうなっているのかも、知る由もない。いつ安全保障上の調査が修正第四条にかかわるかの法を全く知りえていないことは、どのような事実の組み合わせを考量したらよいのかの判断について、裁判所を傍観者のままにさせている。裁判所は、人権の鍵だとして柔軟に修正第四条の令状主義を解釈してきた。それは理論的には成熟しても、実務では不確かな部分を残した。安全保障の領域では、刑事司法での役割と必ずしも同じわけにはいくまい。⁽²¹⁰⁾

安全保障上の利益が絡む捜索に令状を必要としかどうかを司法権が判断するとき、個人の人權（これは司法権の得意とする分野）と安全保障の利益や意義を衡量しなければならないところ、法に基準が設けられていないこともあって、裁判官は能力的にも判断しづらいようだ。かかる基準を示す立法が必要で、議会にこれを制定する義務があるように思われる。

（2）大統領の安全保障権限の統制

海外の諜報活動に関連した国内の捜索は、FISAでFISCtの許可があればできる。すでにみたように、FISCtは、電子的監視の対象が外国政府またはその機関であると信じるに足る相当の理由（probable cause）があれば、

これを認める (50 U.S.C. § 1805 (a) (3))。かかる情報とは合衆国の、(A) 外国勢力またはその機関の現実もしくは潜在的な攻撃その他の重大な敵対行為、(B) 外国勢力またはその機関による破壊工作または国際テロ、(C) 外国勢力またはその機関の諜報ネットワークによる秘密裏の諜報活動、から保護するのに必要なもの、とある (50 U.S.C. § 1801 (c) (1))。FISCt は憲法三条の裁判所である。電子的監視や盗聴は外国の政府やテロ集団との交信に限られるけれども、FISCt の許可を要件としたのは、ここで人権保障の防波堤を考え、そこでの蓄積を電子的監視の許可の法的基準とする目論見があつたのであり、その意味では安全保障の搜索にも修正第四条の精神は生きていゝといえる。⁽²¹⁾ 伸縮

FISCt の審理は非公開である。法は、FISCt や FISC R の審理記録は、「最高裁長官が法務長官と DNI との協議で定めたセキュリティの手法の下で維持されるものとする」としている (50 U.S.C. § 1803 (c))。一九七九年に Warren Burger 最高裁長官がこれを策定している。それらがいかなるものであるうとも、FISCt はセキュリティに必要と合理的に判断する手続を定めうる (§ 1803 (g))。二〇一〇年一月一日に、FISCt の個別的な手続は E.O. 13526 「秘密指定安全保障情報 (Classified National Security Information)」に服する⁽²²⁾と相成る。一般に、秘密指定された情報は二五年後に自動的に審査に服するが、FISA のファイルは五〇年間、原則として、審査に服することはない。⁽²³⁾ 当然 FOIA (情報公開法) に基づく公開請求がなされるけれども、執行権側は、安全保障の諸決定には憲法二条によって大統領に完全な裁量権があり、それはその情報管理権にも及ぶとする。もつとも、憲法はこの点明確ではなく、立法で規定すれば大統領はこれに服すべきとの解釈もあり、議会と大統領は安全保障の情報へのアクセスには権限を共有しているとされる。⁽²⁴⁾ ここにも権力分立が問題になるのをみるのである。

キースは安全保障上の搜索にも令状主義は及ぶとした。その前年、第六控訴裁判所は、完全に国内であれば、修正

第四条の令状主義から安全保障は免れることはないとしていた。⁽²⁵⁾ただキースをはじめ裁判所は、海外の安全保障上の搜索に適用されるかは判断していない。パウエルはキースが国際的な安全保障活動に及ぶとは述べていない（及ばないともっていない）。これは立法に委ねたのであり、FISAが制定されたとき、きれいに整理できる。

もっとも、諜報機関にあつて、FBIもCIAも国内のテロをはじめとする安全保障上の諜報にこうした区別を嚴格に認識しているかは疑問である。キースでは令状主義を貫徹させたが、どのような令状がどのような場合に必要なのかは立法もなく、コンセンサスがない状態である。⁽²⁶⁾そんな中で実務だけが先行している感がある。実際、安全保障としての諜報を国外と国内に嚴格に区別できるかは疑問ともされよう。⁽²⁷⁾

外国の安全保障の脅威に対抗するため国内で電子的監視をするのに、修正第四条が適用されるか。これは明らかに否定されるところの強い論調がある。⁽²⁸⁾修正第四条の令状主義は、外国の脅威から安全保障するのに監視がなされるときには、必ずしも適用されないとするのだ。テロリストには二つの別々の法システムで対応される。一つは、通常の刑事司法の枠内で、憲法三条の司法権の判事が相当の理由（probable cause）を認める証拠を提示しなければならぬ。もう一つは戦時で、外的脅威から安全保障するために監視に要する令状を政府も軍隊も必要としない。「合衆国内での軍事作戦も、国外でそうであるように、国家安全保障を守るために同法的自由を一般に受容する」。

安全保障と諜報はアメリカ建国から密接につながり、国家の重要な責務であつた。⁽²⁹⁾初代大統領ワシントンはこう述べている。「よき諜報を調達しなければならぬことは明白であつて、議論の余地はない。私が付け加えるべきことはただひとつ、汝、万事をできるかぎり秘密にせよ。この種の多くの企ての成功は秘密にあり、それなくしては大方敗北することになるからだ」。⁽²⁰⁾

そもそも、安全保障のための諜報活動は憲法上誰の権限とされるのか。議会だとすれば大統領の諜報活動には厳格な法律の根拠が必要であらう。フェデリリスト・ペーパーでジェイは以下のように述べている。⁽²²¹⁾ 完全な秘密と迅速な派遣が時として必須であるのは、いかなる性質のものであれ条約の交渉にはつきものである。もつとも、有益な諜報は、もしそれを持っている人が発見される心配を除去してやれるなら、獲得できる場合がある。大統領の秘密を頼みにし、上院の秘密を信頼せず、ましてや大所帯の下院の秘密など信用しない者も多数いる。大統領は条約の締結に上院の助言と承認で行動する一方で、分別が論すような手法で諜報の業務に取り掛かることができるのである、と。外交と諜報は大統領の排他的関心なのだと考えは、建国まもない時代での微妙な歳出をめぐって争っていた議会と大統領の間ではすでに共有されていた。⁽²²²⁾

令状なしで盗聴を行っていた歴史は浅くない。一九七〇年代の政府の諜報活動を洗いだした連邦議会のチャーチ委員会⁽²²³⁾はこう述べている。「一九三〇年代来、諜報機関はしばしば盗聴を行い、司法令状の便益なくしてアメリカ市民に盗聴器を仕掛けてきた。…こうした監視のこれまでの対象は、連邦議会議員、議員秘書官、ジャーナリスト、報道者、そのほか、犯罪行為にはかかわっておらず、ホワイトハウスの国内問題顧問やベトナム戦争後の反対グループのような、国家安全保障に本質的な脅威を持たない多くの個人や集団を含む」。ここで注意すべきは、安全保障の名目であっても、それは反体制グループなどをターゲットにして、政治目的でなされているということである。刑事捜査と異なり、安全保障とした場合の目的や利益は必ずしも一義的ではない。

国内も含む安全保障は大統領の権限であり、そのための必要な情報を収集できる固有の権利を大統領は有するとの憲法解釈に立てば、キースも不当とみることになる。ただキースは最高裁判決であって、立法ではない。外敵の脅

威から安全を保障するための諜報などを含む電子的監視については、最高裁は判断していないけれども、立法で許可を必要としており、大統領に安全保障の固有の権限を認めれば、FISAは違憲となろう。この点、FISA以前に、大統領は平時にあって、自らの権限に基づいて安全保障となる交信をモニターしていたとし、FISAの令状は修正第四条の令状ではなく、政府の行為が合理的であることのみを要求するもので、相当の理由ではないのであり、それは一種の手続で妥協的産物とされる。⁽²²⁵⁾ その意味で大統領固有権説に立つても、FISAは大統領権限を制限するのではなく、その行使の手続を定めたにすぎないと解すれば、FISAは違憲とはならない。⁽²²⁶⁾

キースは、ニクソンの大統領固有権限論が少なくとも国内の安全保障の諜報には修正第四条を凌駕しないと判断した。ニクソンは帝王的大統領(Imperial Presidency)のピークともされ、大統領の安全保障権限の優勢を強調した一方で、議会にはこれをコントロールする動きが見られた。一九七三年の戦争権限法はその典型である。⁽²²⁷⁾ 一九七八年に制定されたFISAも、こうした大統領権限を議会が制御する一環とみられる。⁽²²⁸⁾ お調子に乗っている大統領に議会がお灸をすえるといったところか。ただこう理解すると、安全保障上の諜報としての電子的監視に令状を要するかどうかは政策の問題であって、憲法問題にはならないととらえることとなる。⁽²²⁹⁾

(3) 修正第四条の対テロの実務への投影

現実には、大統領に広範な安全保障権限が認められている。大統領(執行権)は、テロとの戦争にあって無令状でアメリカ国民とテロの疑いのある外国人(国や団体を含む)の電子交信を監視している。ブッシュ43は九・一一の後、AUMF(対テロのために武力行使を含むあらゆる権限を授権する議会決議)に基づいて、NSAによるテロ監視プログラ

ム (Terrorist Surveillance Program (TSP)) を立ち上げている。

これには、修正第四条に反する大統領権限の行使だとの批判がある。⁽²³⁰⁾ TSP の中身は、ニューヨークタイムズ紙がすっぱ抜いたことで、その存在が明らかになったものの、公刊されておらない。ACLU (アメリカ人権協会) が起こした訴訟で、TSP では、一方当事者が国外にいて、NSA がアルカイダやアルカイダに関連する組織のメンバーもしくはその支援者であると結論するに合理的な根拠を持つ電話や E メールをカバーしていることが明らかとなっている。⁽²³¹⁾ ブッシュ 43 側は、TSP は修正第四条には反しないとしており、それは安全保障に関する諜報は大統領固有の権限であることと、NSA による監視は合理的であることをあげる。⁽²³²⁾

国内の安全保障に関する諜報としての電子的監視に、キースは執行権の独断のみで行ってはならないとした。海外の諜報活動には修正第四条は及ばないと断定した最高裁判決はない一方で、下級審は大統領の安全保障権限を認めている。ただ、その分野で執行権に濫用がみられ、チャーチ委員会をはじめ、議会の統制が必要だと認識されるようになり、FISA を制定して、司法的監視をビルト・インさせた。もともと、現実には FBI や NSA は国内での安全保障目的で電子的監視を行っており、問題となっている。⁽²³³⁾ その際、執行権は、キースでは温存された大統領の固有権を前面に出して正当性を主張するのである。

キースは確かに、タイトル・スリーが安全保障に必要と判断する大統領の措置権限に影響を与えるものではない (U.S.C. § 2511 (3)、現在削除) と断言している。しかし、これはいかなる権限をも大統領に与えるものではない。文言はあくまで中立であり、単に大統領の憲法上の権限を制限するように解されてはならないとするもので、「要するに、議会は単純に大統領の権限を議会がそうだと判断するところに委ねた」。⁽²³⁴⁾

この問題は、安全保障権限は憲法上大統領に専権が認められているか、そうではなくそれには立法の根拠が必要だとするかで、解釈が分かれる。⁽²³⁵⁾ 政策として安全保障には秘密や効率が高度に求められると考えれば、外的関与としての議会の同意はこれをそぐということになるし、一方で法の支配や民主性、公的支持を要するとすれば、そうはならない。いずれにせよ、FISAがそうであるように、安全保障としての電子的監視には議会への報告が大統領に義務づけられており、大統領などの命令は正式の書式で出すなど、アカウンタビリティは要請されている。⁽²³⁶⁾ もっとも、FISAは、大統領固有権限論者からすれば、これを規制する法で違憲だと主張される。そう考えると、FISAは議会と大統領の妥協の産物ともいえる。⁽²³⁷⁾

大統領は安全保障のための情報収集の権限を有する。これは判例である。⁽²³⁸⁾ ただそうだとすると、憲法上の人権を侵してまで許されるわけではない。大統領にかかる権限が憲法上認められると解するとき、そこに立法の根拠は必要なのか、どこまで規制できるのかの困難な問題が生じる。どの人をターゲットにするか、いかなる手法を選択するかの判断は執行権にあらう。しかし、監視の手法の選択肢や手続は立法で規定すべきであり、その立法にのっとって行われなければならないまい。FBIやNSA、CIAなどの諜報には、立法よりも大統領命令や法務長官の通達が手続の主たる法的根拠とされ、立法の関与ははなはだ弱い。⁽²³⁹⁾ 問題は事後的に諜報活動をどこまで公表すべきかである。事前の公表は性質上免除されうる。それが免除される場合を総合衡量によって判断していくのが法とならう。⁽²⁴⁰⁾

連邦犯罪の捜査やそれによる刑事訴追も、そして内外の諜報活動も、憲法上執行権（大統領）の権限である。大統領権といっても制定法に服するのであり、判例の蓄積もあって、両方とも制定法が大統領のこうした権限の行使を規制している。ただ安全保障のための情報収集、さらに電子的監視は、刑事司法と多くの点で異なり、修正第四条の令

状や搜索押収の要件は緩和される。刑事事件とは違って、安全保障では情報を収集するターゲットは必ずしも特定できず、しかも極秘が要求される。そのため、司法を迂回することはおろか、一切公表されることなく、秘密裏に政府諜報機関のエキスパートが行っている。そこには、修正第四条との整合性の憲法問題が提起されう⁽²⁴⁾る。他方、かかる権限は大統領固有の権限であって、大統領の判断でなしうとの憲法的主張もある。FISAのように、制定法があればそれに大統領は拘束される。しかし、それがカバーしないところで、しかも執行権の責任ある判断で安全保障上必要であるとされれば、大統領権限で実行される。

修正第四条（令状主義条項）が安全保障の捜査には控えめな（*hedge*）機能しか果たさないのは、大統領の安全保障権限の憲法上の定位もさることながら、修正第四条自体にあるともいえよう⁽²⁵⁾。これまで見たように、最高裁は同条の安全保障上の捜査への射程は明確にしていない。同条の令状主義は順応的（*malleable*）に解釈されてきた。令状がどのような場合に必要なのか、そしていかなる令状が必要なのかは、鶏と卵の問題であって憲法上オープンで、加えて安全保障では、司法権はいかなる基準を適用すべきかには不案内であり、事実上照らしてどのような衡量の判断をすればよいのかも定かでない⁽²⁶⁾。

安全保障のための電子的監視の手法として制定法が認めているものがある。一つは安全保障請求状（National Security Letters）である⁽²⁴⁾。もうひとつは三〇〇以上あるといわれる行政文書提出命令（administrative subpoena）である。これらは直接、盗聴など行うのではなく、交信記録等をFBIなどに提出させるよう、民間に命じるものである。大統領の安全保障権限が声高に叫ばれるのが、NSAによる電子的監視である。チャーチ委員会はすでに、NSAが国内諜報で問題となることを指摘していた。いわく、「危険は、NSAの国内の交信に対して驚くようなテクノロジー

を向ける能力にある。∴NSAは内に転回されて、われわれ自身の人民に対して使用されるだろう⁽²⁴⁵⁾。NSA自体制定法に基づく機関ではなく、その活動にも立法的規制はほとんどない。NSAの活動のための権限に立法的根拠はない⁽²⁴⁶⁾。まさに修正第四条とは別の世界で、大統領の憲法二条の権能に基づいてのみなされる。安全保障の名の下でのNSAの諜報活動を考察することは、大統領の権限を考える格好の素材となる。

五 国家安全保障局（NSA）の電子的監視と修正第四条

1 NSAによる電子的監視とその現状

(1) ^{メタデータ} metadataとアメリカ人の秘密理の諜報活動

キースは明言を避けているが、これをうけて制定されたFISAは、外国の諜報活動の電子的監視を執行権に授けられた。九・一一以降、ブッシュ43はNSAに、一方当事者がアメリカ国外にいて、通話の参加者が「アルカイダもしくはその提携団体のメンバーもしくはエージェントであると合理的に信じられる」場合、無令状で電子的監視を行えるようにした⁽²⁴⁷⁾。

二〇〇八年のFISA改正法は、これまでのFISAの手法を凌駕する、新規かつ独立の諜報収集権限を根拠づけた⁽²⁴⁸⁾。それがFISA七〇一条(50 USC §1881a)で、海外にいる非アメリカ人をターゲットにする諜報に政府がFISCの授權を求めることを容易にした。その際、それまでFISAでは政府はターゲットが外国勢力あるいはその機関であるとする相当の理由(probable cause)を立証しなければならなかった。これが不要とされ、政府はター

ゲットにする場所や性質などを特定する必要がなくなったのである。

本稿冒頭でふれたように、ボストン・マラソン事件で顕著になってきたのは、生粋の国内のテロリストをどう監視するか、いわゆる一匹狼 (lone wolf) の問題である。国内にあって安全保障目的での秘密裏の監視を大統領権限で行うことができるかである。

大統領がNSAを通じて国内で電子的監視を行っていることが暴露されている。先に見たスノーデンの暴露が引き金となって、NSAが国内のアメリカ人の電子的監視を行っていたことが明らかとなってきた。友好国であるドイツのメルケル首相の携帯電話までNSAがフォローしていたことも、彼が明らかにしている。⁽²⁹⁾

二〇一三年夏に問題となったのは、NSAが、国際のみならず国内での電話の交信の記録を大量に収集していたことである。加えてインターネット交信の傍受を、一次的には国外にいる外国人をターゲットにしているが、アメリカ人の交信も偶発的に収集してしまっているのである。むやみな大量のデータ収集は、なるほど対テロ等安全保障のための諜報として役立つ面もある。しかし、反射的に順法の無垢の市民のプライバシー情報をも収集することになり、憲法上看過しえなくなる。政府は、これは愛国者法二一五条もしくはFISA七〇二条に基づくもので、合法としている。

二〇〇六年から、FBIは定期的に更新する、主要な電話会社からの大量の電話記録を極秘に収集しており、Eメールやインターネット検索に関する情報も同じように収集していたことが明らかとなっている。その間、グーグル、フェイスブック、スカイプ、アップルを含む九つの主要なインターネット会社のデータを、収集するようになっていく。これはPRISM^{ブルイスメ}といわれるコンピュータ・ネットワークで簡単にできるようになっている。データはNSAを

はじめICで共有されることもある。

電話の記録の収集は愛国者法二一五条に基づく。FISAのいう「業務記録 (business records)」であるから、FISCtの許可によって国際テロに関連する (relevant) と判断される有体物 (tangible things) に第三者を通して秘密にアクセスできる。プリズムは、二〇〇八年に制定され二〇一二年の再授權されたFISA七〇二条に基づくとしている。国外の非アメリカ人をターゲットにするもので、そうすることとテロに関連していることの二つの要件を充たしていることが合理的に信じられればよいとする。

プリズムは^{メタデータ}metadata⁽²⁰⁾を収集する。それはFISCtの命令に基づき、誰が誰に電話したか、その電話番号は何か、その日時や通話時間のデータであって、通話の内容はもちろん、場所の情報も含まれない。NSAから請求を受けた電話会社はデイリーベースでこうした情報を提供し、これをNSAが^{集積庫}Collection Store^庫となつてデータベース化する。FISCtの命令では、収集してから五年以内に削除されるものとされる。NSAは、この命令を得るためにFISCtに対して、当該電話記録に「明瞭にできる合理的な疑い (reasonable articulable suspicion : RAS)」のあることを立証する。RASは、一般的な搜索に必要とされる「相当な理由 (probable cause)」ほど厳格ではない。

無作為で大量の、そして秘密の、NSAによる情報収集が懸念されている。重要なのはその活動の監視 (oversight) にある。現行法はこれを用意している。なによりも、FISAは捜査にはFISCtの承認を法律要件としている。申請の数は年々増加している (二〇〇九年は二件だったのが、二〇一二年には二二件となっている) 一方で、二〇一二年には申請を否定したケースは一件もなかった。FISA七〇二条では、プリズムを意識して、個別の監視命令を取得するのに事前のFISCtの承認は不要とされた。同条はそうしたプログラムの実施にはFISCtの重要な意見

もいれて議会（諜報司法委員会）に報告する義務があるが、一般に秘密とされる。

政府は、NSAのメタデータの収集もプリズムも、すべて法令にのっとった適法なものであることを強調する。⁽²⁵¹⁾しかし、こうした既存のメカニズムでは濫用は十分に統制できない。NSAは通信会社から「好きなものは何でも引き出せる（pull anything it likes）」とまで認識されている状況が、そこにはある。

（2）オバマ大統領による改革

スノーデンは秘密を漏洩した犯罪者として、司法の手に委ねられるべきとの声は強い。⁽²⁵²⁾他方、この暴露でNSAによる国内の市民向けの電子的監視が露見し、大統領をしてチェックが必要だと感じせしめるにいたった。オバマは、大統領の諮問機関「諜報とコミュニケーション技術に関する研究会（President's Review Group on Intelligence and Communications Technologies）」を立ち上げ、二〇一三年二月二日、三〇八頁からなる最終報告書『変化する世界における自由と安全保障』⁽²⁵³⁾を公刊している。

そこでは、アメリカの民主主義は自由と安全保障の二つの価値を同時に追求するものであり、そのバランスをどうとるかが重要だとしたうえで、「われわれの安全保障の脅威に対して国民を保護すること」、「他の安全保障や外交政策の利益を保護すること」、「プライバシー権を保護すること」、「民主主義、市民的自由、法の支配を保護すること」、「ネットワーク世界の繁栄と安全と公開性を促進すること」、「戦略上の同盟国を保護すること」、の諸目的を明確に掲げる。そして次の四つの原理を確認する。第一に、「政府は、二つの異なった安全の形態、国家の安全保障と個人のプライバシーを同時に保護しなければならない」。第二に、「中心となる仕事は一つの危機管理（risk management）で

ある。多様な危機が巻き込まれており、そうしたもののすべてが斟酌されなければならない」。第三に、「balancing」の考えは確かに重要な要素であるが、同時に不適切で誤った方向に導く（misleading）。第四に、「政府はその諸決定を、コストとベネフィットの両方を含む結果の慎重な分析に基づかせなければならない」。

そのうえで、立法の制定や改正を含む四六の提言（recommendations）を行う。主に、愛国者法二二五条での大量の電話のメタデータ収集をやめさせること、透明性を確保すること、非アメリカ市民のプライバシーを向上させること、官邸の審査やFISCtの改革を含む組織改編を行うこと、などである。

この報告書の関心は次の六つにある。第一に、アメリカ人に対する監視で、愛国者法二二五条を適用してNSAがこうした収集を行っているのを懸念し、議会がそうしたデータの蓄積をやめさせ、そうしたデータが個別に、いつ安全保障の必要性があるかを政府が問えるようにするシステムに移行させるべきとする。第二に、非アメリカ市民のプライバシーにも配慮すべきとし、法律で特別に認められ、さらに政府が特別のやむに已まれない必要性を示さない限り、アメリカ市民と同様に扱うべきとする。第三に、不当あるいは不必要な監視は避けなければならない。第四に組織の改編を訴える。NSAに関して、その長は上院の同意を要する職とし、文民にも門戸を開くべしとする。次のNSA長官は文民にするよう大統領は配慮すべきだという。これまでのプライバシー市民的自由監視委員会（Privacy and Civil Liberties Oversight Board）に代わって、強化された独立の市民的自由プライバシー保護委員会（Civil Liberties and Privacy Protection Board）を創設せよとする。FISCtに関しても、ここでは政府関係者のみが当事者であるが、議会は新たにFISCtの前でプライバシーや市民的自由の利益を代表できる公益弁護人（Public Interest Advocate）を

創設すべきとする。第五に、地球的規模の交信の技術 (Global Communications Technology) を推進させ、その際、プライバシーや市民的自由に配慮しなければならないとする。第六に、収集したデータをしっかりと保護すべしとする。insider threats (組織内脅威) に伴うリスクを軽減せよというのである。政府は限定された機関でのみの共有を訴えるが、セキュリティ・クリアランスを厳しくしたり、監視の制度を設けたりと、マネージメントの改革が必要とされる。

スノーデンの暴露以降、諜報機関、とりわけNSAの国内の電子的交信の秘密の監視が世論の関心を呼ぶ。オバマ大統領はこれを認めたくて、アカウンタビリティの観点から国民向けの応答を公言しており、さらに議会も関心を持つに至る。法的問題では、FISAを改正した愛国者法二一五条とFISA七〇二条にその注意が集中した。⁽²⁵⁴⁾

オバマ大統領は四〇分以上にも及ぶ、電子的監視に関する初の主要な演説を二〇一四年一月一七日に行った。⁽²⁵⁵⁾ アメリカは、安全保障に脅威を及ぼさない一般市民には諜報活動をしていないことを改めて強調する一方で、安全保障、特に反テロとして諜報や防諜活動は不可欠で、⁽²⁵⁶⁾ 発展したテクノロジーに裏付けられてデジタルのコミュニケーションに入りこんでいかなければならないとした。ただそこには制約があり、法の支配に基づき、安全保障上の必要性が確実であるときのみ行い、人権を最大限に尊重する。そのためにチェックや防御のシステムを充実させるとしている。同日に出された大統領政策指令では、⁽²⁵⁸⁾ これまでのような大量の (bulk) 収集はやめ、諜報など限定された正当な目的でのみ行い、大統領安全保障補佐官補やDNIによる年次ごとの定期的な審査や調整を行う。収集を実施したときは、一定期間内にDNIに報告する義務を課している。取得した情報の流布や留保にもルールを設けている。この大統領の指令は、NSAによる電子的監視について法的ルールを整理したものといえよう。

2 NSAの組織と法

NSAによる電子的監視は法的にどう正当化できるのか。一九五二年一月四日、トルーマンの大統領命令によつて国防省に設置されたNSAは、暗号や記号を解析する諜報機関である。⁽²⁵⁹⁾第二次大戦中、日本やドイツの暗号を解読する重要性を認識したことに由来する。NSA/CSS (Central Security Service) は、^{情報源}SIGINT (Signals Intelligence) とIA (Information Assurance) の果実と役務の両方を含む暗号作成 (cryptology) で政府をリードし、あらゆる状況で国家と同盟国に有利な決定を得るためにコンピュータ・ネットワーク作戦 (Computer Network Operations) を可能にさせる。IAとは、「センシティブなあるいは秘密の安全保障上の情報に、外国の敵対者がアクセスできないようにする」任務で、SIGINTとは「諜報及び防諜のため、そして軍事作戦を支援するために、外国の信号から諜報の情報を収集し、加工し、流布させる」任務である。NSAはまた、憲法や法令の範囲内で人権を侵害しないように、国内外のテロリストやその組織を打ち負かすべく、ネットワーク上の戦闘作戦 (Network Warfare Operations) を可能にする。

一九七二年一月一七日の「信号諜報 (Signals Intelligence)」と題するNSC (国家安全保障会議) 諜報指令第六号は、中央諜報管理部部长 (Director of Central Intelligence Board) が確立させた目的や要件ならびに優先順位に従つて、NSAがSIGINTをなすこととする。SIGINTは^{交信の諜報}COMINTと^{電子諜報}ELINTからなる。COMINTは、無線などによる外国の交信を傍受してデータ処理する活動である。もともと軍の諜報機関の機能であつたELINTは、交

信外や電磁波からくる諜報目的の情報を収集し処理する。

NSAはICにあって最も秘密性が高い。前身は国防省に設けられ統合参謀長の指揮の下におかれた軍安全保障局 (Armed Forces Security Agency (AFSA))²⁶⁰で、ジョンソン大統領が署名した統合参謀長指令 (JCS Directive) 二〇一〇によって、一九四九年五月二〇日に設置された。一九五二年一〇月二四日、トルーマンの「交信諜報活動 (Communications Intelligence Activities)」と題する極秘メモがNSC諜報指令第九号となり、これによってAFSAが廃されてNSAが設置される。ただし、NSAの存在は一九五七年まで公に知られることはなかった。国防省内で別に組織されて、安全保障に高度な特別の技術的調整的機能を発揮した。NSAの設置根拠 (Chattel) はNSC諜報指令第六号であり、NSAにSIGINTを命じている。

一九八一年一二月四日に発せられたEO 12333は、NSA/CSSの権限の輪郭を規定している (1.12(b))。それは、国家や国防省の任務を支援するために、外国の諜報や防諜の目的で信号の諜報の情報やデータを収集し (秘密の行動を含む)、加工し、分析し、生産し、流布させることである。二〇〇八年七月三二日に改定されたEO 12333は、二〇〇四年の諜報改革テロ防止法や九・一一委員会の答申、さらにDNIなどの諜報機関の長に従うことが明記される。ただ外国の諜報の情報収集のため、国内で市民を含む電子的監視はFISAに従う。それまでは法の根拠なく電信の諜報を行っていた。二〇一三年四月、FISCがVerizon^{ヴェリゾン}に対して三か月ごとの各発信者による電話の情報を提供する命令を出していることが公にされ、ほぼ同様に、AT&TやSprint^{スプリント}などに対して七年以上も交信情報の提供が命じられている。そしてプリズムである。大量のメタデータの収集が、NSA (FBIも含む) によってなされている。⁽²⁶⁰⁾

政府は、この収集はFISAに基づいて行われた合法的なものであるとした。その濫用や違法性の統制はFISCIで担保される。FISCIの判事が、大量の収集は許可されていらないとするなど、NSAとの間に相当の温度差があり、根本的な見解の違いも浮き彫りになっている⁽²⁶¹⁾。NSAは、テロリストはGoogle^{グーグル}などを通して交信していると、法を破る意図など毛頭ないとしているけれども、大量の収集やテクノロジーが問題となっている面もある。

NSAは現在三万人以上の職員を要し、その多くは数学者である。一二〇カ国以上の言語分析者もいるが、職員の半分以上は軍人である。その責務は、SIGINTとIAの二つである。前者は電信にのつかった声やインターネット交信、その他信号を外国の諜報や防諜の目的で収集し分析し伝達させるものである。IAとは、軍事を含む政府の交信や情報のストックといった秘密保持システムを保護することである。このようにNSAは、国防省とICの両方のメンバーとしての責務を果たして、戦闘支援の機能を持った機関と国家諜報機関を兼備する⁽²⁶²⁾。

これまでみたように、諜報のための電子的監視は愛国者法とそのさらなる改正によって、執行権の便宜に改革されている。FISA七〇二条は、ターゲットが外国勢力であることが明らかであれば、FISCIの事前の許可なく電子的監視ができるようにした。FISAは電子的監視に司法的統制を加えることを目論むが、それは踏まないのである。なるほどアメリカ市民がターゲットにされることはない⁽²⁶³⁾。しかし、多くのアメリカ人のメールや交信記録がそのプロセスで偶発的に(incidental)収集される危険は払拭できない⁽²⁶⁴⁾。FISCIの役割は、政府が交信を将来、標的を絞って収集すると提案している、最小限の手続を審査することに限定されるけれども、こうした標的がアメリカ市民に絞られていないか、最小限の手続を履行しているかを見極めなければならぬ⁽²⁶⁵⁾。

愛国者法二一五条も、記録がテロや秘密の諜報からの防御のための捜査の一環であれば、ターゲットが外国勢力だ

との立証は不要としており、メタデータが無造作に収集される可能性が増している。二〇〇六年以降、電話のメタデータがこの二一五条に基づいて大量に収集される。すなわち、FISCtによって「関連する (relevant)」と判断された有体物の作成を個人に命じる権限が授権される。

NSAは大量で集める方が効率的であり、公にされた五四のテロ事犯で一三がアメリカとコネクションを持ち、その一二に電話のメタデータが奏功したとしている。⁽²⁶⁶⁾ 安全保障捜査の基本である秘密性と情報社会の宿命だとし、かつまた法令に従ったもので、NSAは遵法精神に厚い文化を持ち、立法に対して直接アカウンタブルであるとして、こうした活動を正当視する者もある。⁽²⁶⁷⁾ FISCtの審査を経ているものであり、このFISCtは決してゴム印の機関になっていないとする者もある。⁽²⁶⁸⁾

実際、大量データ (Big Data) の偏在はその効用が故にであり、技術の発達は大量データの有用性を自覚せざるを得ないのであって、問題はむしろ、誰によってどのように大量データが使われるかにあるともいわれる。⁽²⁶⁹⁾ スノーデンの暴露であからさまになったNSAのこの活動は、不合理な搜索に当たり、憲法問題も絡んで議会人や専門家の関心をわかに集めることとなる。

3 NSAによる電子的監視の違憲性

NSAのこうした活動は勢い、修正第四条との抵触が疑われる。その根拠となる愛国者法二一五条あるいはFISA七〇二条が修正第四条に反するとして、憲法訴訟になる。アメリカ保護法そして二〇〇八年FISA改正法で設けられた規定は、電子的監視を立法で明確にし、司法的授権に基づかせるとともに議会の監視に服させ、修正第四条に

反しないように配慮している。これにのつとつて、国外にいると信じられる者の外国諜報は無令状で監視できるとした規定が、以下にみる *Klayman* 事件と *Clapper* 事件で問題となった。

この憲法訴訟を最初に判断するのは *FISCt* である。 *FISCt* は、このメタデータ収集にはスミス法理（第三者の法理）から修正第四条の障害はなく、個人に修正第四条の利益が見出されない以上、同じような状況にある個人の膨大な番号と一緒に収集しても、そもそも無であつた（*ex nihilo*）ものからはなにも生じないのであつて、結果、修正第四条に反しないとした⁽²⁷⁰⁾。

二〇一三年二月一六日、DC 連邦地裁は *NSA* の電話等の電子交信の情報収集プログラムを違憲とする判断を行った（*クレイマン事件*）⁽²⁷¹⁾。アメリカ市民の電話記録のメタデータ収集の慣行は適法（憲法）かが争われた。本件では *FISCt* の判断を経ている。ブッシュ43が任命した *Richard J. Leon* 判事は、行政手続法での訴訟は *FISA* が司法審査規定を設けていることから認められないとするも、憲法判断の原告適格は認め、この慣行は五年という長い期間でデータが収集され加工される点で、その他の電話交信記録（*benign*）などとは大きく異なり、また歴史的コンタクトの情報がないものとも異なつて、テロとの戦いが終わるまで続けられる可能性が十分にあるとした⁽²⁷²⁾。電話や電子交信は、技術の発達した今日、数十年前と比較にならないほど多くの市民の間に浸透しているとして、プライバシーを侵しており、修正第四条に反するとした。政府側は「特別の必要性」を主張したが、立件できていないとして退けている⁽²⁷³⁾。

ここではメタデータがプライバシーの保護の対象となるかが、先ず争点となろう。 *NSA* 長官 *Keith Alexander* は、メタデータは電話の発着のデータであつて、電話で何をいったかではない点を *CBS* の番組で強調した⁽²⁷⁴⁾。レオン判事

は、それが歴史的に蓄積されることと、現在の電話は発信地など電話の記録以外の情報もわかってしまうことから、プライバシーとして合理的な期待を持ちうる⁽²⁵⁾としている。すなわち、スミス判決の第三者法理は pen-register のようなタイプには適用されるが、本件はそれではなく、いわゆるモザイク法理に従ったのである⁽²⁶⁾。ジョーンズでの法理である。それは、個人の車に取り付けられた物理的なGPS装置がこれに付随する情報を巻き込んで収集することとなり、修正第四条の搜索に該当することとなるとした。短期の搜索ならともかく、長期にわたるそうした収集は、家族や政治や宗教や性的な結合の情報も量的には収集されることとなり、修正第四条から司法権の関心となる。

では本件のメタデータ収集は修正第四条のもとで合理的か。愛国者法二一五条は令状を要求してもいなければ相当の理由も要求していないから、特別の必要性 (special need) で正当化されるかを検討する。特別の必要性は、先にもたように、令状や相当の理由を要求することが現実的ではなく、通常の法執行の必要性をこえる、特別の必要性がある場合であり、かつそうした場合でも、政府利益とプライバシーを衡量しなければならない⁽²⁷⁾。すなわち、①本件搜索で侵害されるプライバシー利益の性質②訴えられている侵害の特質③政府利害の急迫性と性質およびそれを充たすための本件手段の効率性、を考量し、本件ではメタデータ収集を実行していくうえでのプライバシー利益が重視されるとした。

この地裁判決から一日後の二月二七日、ニューヨーク連邦地裁は逆に、スノーデンが暴露したNSAの国内電話データの大量収集は合法とした(クラッパー事件)⁽²⁸⁾。ポーリー判事は、FISAの規定はむしろ政府の権限を法治主義的に根拠づけると同時に制限するものであるし、安全保障の領域では司法は委譲せざるをえず、FISCtなどもNSAのこうしたことを認めており、またテロの事前抑止に機能した実績もあるとする。大量収集に無垢の人の情報

が入り込んでしまう危険が指摘されるが、大容量のメタデータでなければ何が関係があり何が関係ないかがわからないという。原告の訴訟要件の認定には積極的であったが、本案の判断では政府に好意的となる。アルカイダの技術も進歩し、遠隔的にテロを行えることを考えると、「大量の電話のメタデータの収集のプログラムは、政府のカウンターパンチを示している。断片的で束の間の交信をアルカイダのテロのネットワークに再構成し除去することにつながるのである」⁽²⁷⁾。スミス判決を踏襲して、本件の電話番号の記録の大量収集は修正第四条に反しなかった⁽²⁸⁾。

なお両事件とも本稿執筆段階（二〇一四年末）では控訴中である⁽²⁹⁾。

4 小 括

国内の諜報活動は修正第四条と正面对決して、法的な議論はつきない。刑事司法には同条の要請があるが、諜報活動には厳格には適用されないとするのが実務といえよう。もっとも、同じ公権力による電子的監視では、刑事司法でも安全保障の諜報でも手法は同じである。根本的に異なる点は、刑事司法が犯罪の発生をうけてそれを遡及的に調査するのに対し、安全保障としての諜報はテロ対策のように、むしろ事の発生を待っていては遅すぎ、それを事前に抑止するために情報収集する将来的（proactive）なものであることである。そこでは刑事手続に関する規定たる修正第四条がどうコミットしてくるのかは、権力分立の憲法原理が絡んで一義的ではない。安全保障には大統領の専権が認められ、修正第四条が及んだり、立法の規制が認められたりすることはないとも論じられる。

この点、ラスコフの議論は興味深い⁽³⁰⁾。彼は国内諜報活動（テロ対策のみに限定されるわけではない）実務とそのガバナンスにギャップがあることを注視し、その原因が理論の欠如、制度の欠陥、概念の未整理にあると指摘する。最高裁

が、キースでもそうであるように、法理論的な指導原理を国内の諜報活動に関しては明確に判示していないことを指摘する。一方で、諜報は福祉国家から当然の帰結であり、それは規制のための情報収集と本質的に異ならないとする。規制は危険察知であり、それは国内の諜報も同じである。すなわち、「規制の政策や実務には十分慣れ親しんだ危険評価 (risk assessment) の一側面として最もよく考えられるのであり、行政国家内で発展した法的制度的道具は効果的で、長続きする諜報のガバナンスの枠組みを創設するのに必要である」とする。⁽²⁸³⁾したがって、基本的には規制法、つまり行政法で国内諜報の枠組みを考えるべきで、司法審査も合理性審査 (rationality review)、すなわち、「費用対効果の拡大した概念での行政法の枠組みで、規制の使命へのコンプライアンスと透明性に担保された多元主義の司法審査が国内諜報のガバナンスの中心的役割になる」とする。⁽²⁸⁴⁾極言すれば、「国内諜報 (その他の危険評価の形態と何ら変わる(285)ところがない) は、単純に国家がその市民の健康と安全に関する意思決定を形作る情報を生成する手段である」とみるのである。

六 むすびにかえて

安全保障の電子的監視は諜報として執行権によってなされる。その憲法上の根拠は、明文の規定はないものの、憲法二条の大統領権限に求められている。大統領の安全保障権限として、秘密の諜報も認められる。それは違憲であってはならない。修正第四条が安全保障捜査に適用されるかは明確ではない。むしろ、外国の諜報には立法がその手続を規定し、アメリカ人への諜報は厳しく制限している。諜報は制定法が根拠づけと制約をおくこととなる。諜報の権

限は大統領権と憲法上観念されるも、立法の規制や根拠が前提となっている。大統領命令も安全保障の捜査の電子的監視に同様な機能を果たしている。なかでもEO 12333は、法令とかぶる部分もあるが、ICにもわたる政府の諜報に関する包括的な規範となっている。

一方で、対テロ政策の喫緊性は微妙な法逸脱の運用を招来せしめている。「安全保障の理由から令状なしの搜索が志向される要因は、「テロとの戦い」でもたらされた今日の情況のもので、やむにやまれないのである」⁽²⁸⁶⁾。安全保障も憲法上の利益であり、人権保障とのバランスが問題になる⁽²⁸⁷⁾。その際、統治機構上の問題として、議会の規制に服さない、大統領に固有の安全保障権限があるかが争点になる。

もとより、安全保障といっても具体的にいかなる法概念かは明確ではない。留意すべきは、安全保障の利益のの名の下で公権力の情報収集に自由な領域が拡大していくことである⁽²⁸⁸⁾。プライバシーや自由は、テロという安全保障上危険な時代にあつて、警察のみならず軍や諜報機関の権限が大きくなるにつれて軽視される嫌いがあり、そうしたなか、独立した司法の役割は大きく、修正第四条はその契機となりうる⁽²⁸⁹⁾。ただ、修正第四条は司法警察や法執行活動を想定しており、安全保障への適用には憲法解釈の作業を要する。それが公権力によるプライバシー侵害を禁じるとの意図であれば、安全保障についても基本的に妥当する。諜報は国家にとって不可欠であり、安全保障の利益を確保するために効率よく行われなければならないし、憲法上の人権を侵してもいけない⁽²⁹⁰⁾。ジレンマである。安全保障の国家利益は極めて重大であるから、目的に比例した合理的な搜索押収は一般には許容されるとの考えを出発点にすべきかもしれない⁽²⁹¹⁾。

政府の安全保障の情報収集、諜報は修正第四条よりも大統領権限で着々と実行され、裁判所もこれに関与するのに

は慎重である⁽²⁹²⁾。憲法としてはこうした公権力をどう統制するか、個人はこれをどう争うか、救済類型はどうかといった問題がある⁽²⁹³⁾。本稿はこうした課題を認識しながら、憲法の理論的レベルの考察を試みたものである。

- (1) 6 BENJAMIN FRANKLIN, *THE PAPERS TO BENJAMIN FRANKLIN*, 238, 242 (Leonard W. Labaree ed., 1963).
- (2) アメリカ法に安全保障 (national security) の明確な法的定義はなく、一義的にし難い。ここではごく一般的に、「国家が、その独立や主権、領土、国民の生命や財産といった、かけがえのない価値を、外敵の脅威から、軍事力によって守る」と観念しておく。杉井敦・星野了俊『防衛大学校で、戦争と安全保障をどう学んだか』(祥伝社新書、二〇一四年)六二頁。なお侵略を各概念とし、これを排除予防するのが安全保障と捉えることもできる。高橋通敏『安全保障序説』(有斐閣、一九六〇年)四頁。特定秘密の保護に関する法律(平成二五年)は、安全保障を「国の存在に関わる外部からの侵略等に対して国家及び国民の安全を保障すること」(第一条)と定義している。
- (3) See, WASH. POST, June 7, 2013, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN, June 5, 2013, *NSA Prism program taps in to user data of Apple, Google and others*, THE GUARDIAN, June 6, 2013; John Greenburg, *Are Americans being 'targeted' for surveillance?* TAMPA BAY TIMES, July 2, 2013. NSAはアメリカ人を含むEメールの記録を外国の諜報の一環として収集し、膨大なファイルにしていた。NSA collects millions of e-mail address books Globally, WASH. POST, Oct. 14, 2013. 問題は誰の情報をとるかといった標的の定め方 (targeting) であり、これには執行権に全て自由が認められるとすれば、憲法問題になる。
- (4) Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008).
- (5) 「国家が外交軍事政策を形成し実行し、安全保障への脅威を取り除くために必要な情報」と定義される。CURTIS A. BRADLEY AND JACK L. GOLDSMITH, *FOREIGN RELATIONS LAW* 271 (4th ed. 2011). 情報と混合した使用や認識もある。小谷賢『インテリジェンス』(ちくま学芸文庫、二〇一二年)第一章。小谷自身、その定義にはアメリカとイギリスでも異なる文脈があるのに注意すべきとしたうえで、「国益のために収集、分析、評価された、外交・安全保障政策における判断のための情報」と定義している。同上書、一八頁。外国に関する情報の収集や分析、評価などからなる製品である点に着目する認識も

ある。土屋大洋『情報による安全保障―ネットワーク時代のインテリジェンス・コミュニティ』（慶應義塾大学出版会、二〇〇七年）一六―二〇頁。またプロダクトとしてのインテリジェンスに着目し、国家安全保障でもビジネスでも、「判断・行動するために必要な知識」と観念する者もある。北岡元『インテリジェンスの歴史―水晶玉を覗こうとする者たち』（慶應義塾大学出版会、二〇〇六年）一一―一七頁。プロセス、成果物、組織、それぞれのインテリジェンスがすべて同時に語られるとする。マーク・ローエンタール／茂田宏監訳『インテリジェンス 機密から政策へ』（慶応義塾大学出版会、二〇一一年）一一頁。インテリジェンス・プロセスは、「政策決定者が情報の必要性を認識する段階から、コミュニティが政策決定者に対し分析したインテリジェンス成果物を提供するまでの段階または局面」であり、彼は、(1)要求の特定(2)収集(3)処理と活用(4)分析と生産(5)配布(6)消費(7)フィードバック、の七つを分析している。同上書、六九頁。本稿では主にプロセス、とりわけ情報収集のインテリジェンスを念頭に置いている。

- (6) D H S 長官 Janet Napolitano は、「パキスタンやソマリアなどからの移民の子孫がアメリカ土壌で育ち、ジハードのウェブサイトに容易にアクセスするなどした自前のテロリスト (homegrown terrorists) が、新しい深刻な、次世代テロの問題だ」としている。DANA PRIEST AND WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE 136 (2011).

- (7) カナダは諜報を国家警察 (RCMP) に長く行わせていたが、一九八四年に CSIS (カナダ安全保障諜報局) を設置し、RCMP の諜報権限を除去してこれに独占させている。富井幸雄『憲法と緊急事態法制 カナダの緊急権』（日本評論社、二〇〇六年）第6章V、参照。

- (8) RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS: INTELLIGENCE REFORM IN THE WAKE OF 9/11 100-101 (2004).

- (9) JEFFREY T. RICHELSON, THE U.S. INTELLIGENCE COMMUNITY 13 (6th ed. 2012). 諜報のタイプには「政治・軍事・科学技術・財政、経済・社会学的の六類型があり、諜報の標的を「国際・地域・国内の三類型に整理している。Id. at 5-7.

- (10) Id. at 17.

- (11) 民主的統制であり、それは指揮 (direction) と監視 (oversight) の二つからなる。指揮は、諜報任務全般での IC への文民による指導であり、監視は、諜報活動の法枠組み、諜報共同体組織、予算、人事の全ての審査が民主的プロセスで同定されることである。Thomas C. Bruneau and Steven C. Boraz, *Intelligence Reform: Balancing Democracy and Effectiveness*, in

- REFORMING INTELLIGENCE 1, 14 (Thomas C. Bruneau and Steven C. Boraz, eds., 2007). そつには憲法の権力分立原理に基づいた、三権各機関の抑制と均衡に根差した協働の監視が施されているのに加え、ICCや機関の内的(内部監察官など)及ぶ外的(メディアやNGOなど)監視も存在する。ただし、執行権による統制(大統領府によるチェックや命令)が最も重要であるとする。Steven C. Boraz, *Executive Privilege: Intelligence Oversight in the United States*, in *id.* at 27.
- (12) John D. Negroponte and Edward M. Wittenstein, *Urgency, Opportunity, and Frustration: Implementing the Intelligence Reform and Terrorism Prevention Act of 2004*, 28 YALE L. & POLY REV. 379 (2010).
- (13) *Id.* at 381. MARSHALL CURTIS ERWIN, INTELLIGENCE ISSUES FOR CONGRESS, CRS REPORT FOR CONGRESS, Apr. 23, 2013, CONGRESSIONAL RESEARCH SERVICE 7-5700, RL33539, at 1.
- (14) *Id.*
- (15) Harry Howe Ransom, *Producing Foreign Intelligence*, in NATIONAL SECURITY AND THE CONSTITUTION: THE IMPACT OF THE POLITICAL SYSTEM 50, 50-51 (George C. Edward III and Wallace Earl Walker, eds., 1989).
- (16) ローエンタール、前掲(5)書「二四五頁以下、第一〇章「監視と説明責任」。課報の監視は大統領と共有されるけれども、「議会は、インテリジェンス政策を形成するに当たり一貫したブレイヤーになっている」とする。同上書、二七八頁。監視に当たる oversight には、「注意深く配慮すること」と、それとは真逆の、見落としや無配慮という意味もあり、議会や行政府はインテリジェンスを監視する際、前者を行つて後者を避けるようにしている。同上書、二四五頁。
- (17) THE FEDERALIST No. 64, at 392-93 (John Jay) (Clinton Rossiter ed., 1961). なお、A・ハシルトン＝J・ジェイ＝J・マディソン／齋藤眞・武則忠見訳『ザ・フェデラリスト』(福村出版、一九九一年)、三二二―三二七頁(第六四篇、J・ジェイ)、参照。
- (18) 「条約締結権は重要なもので、とりわけそれが戦争や講和、そして通商に関連するものであるからだ。したがつて、それは委任されてはならないだけでなく、最高次の安全保障を与えることになる以上、公共の善に最も伝導性(conductive)のあるやり方で、かつその目的に最も適した人物によつて行使されるようなモードと慎重さをもつてなされなければならない」。
- THE FEDERALIST No. 64, at 390 (John Jay) (Clinton Rossiter ed., 1961).
- (19) 修正第三条の意義については、富井幸雄「軍の私人宅宿営の禁止―合衆国憲法修正第三条の意義」大東文化大学紀要(社

会科学》三九号七三頁、二〇〇一年。軍の権限を規制する憲法規定はこれしかない。もっとも、軍隊の権能については議会がコントロールできる仕組みとなっている。U.S. CONST. Art. I, § 8, cls. 11-16. 軍の法執行活動を禁じた Posse Comitatus Act はその例である。富井幸雄「軍の警察活動の制約—Posse Comitatus 法」法学新報 一一一巻五・六号一六三頁、一一・一二号五三頁、二〇〇五年、参照。

- (20) THOMAS COOLEY, TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 299-300 (1st ed. 1868). そのあとでクリーリーは個人のプライバシー (one's privacy) に言及する。Id. at 305. 搜索押収の令状は犯罪が行われたとの証拠の存在に確信があるときのみ発給され、そのときでさえ「個人のプライバシーを侵してはならない」とする。ただ、プライバシーの何たるかは説明がない。

- (21) *Boyd v. United States*, 116 U.S. 616, 625 (1885). 修正第四条では、個人の家と生活のプライバシーへの侵害から保護されることになっている。Id. at 630. なお、イギリスの経験や歴史から、アメリカ制憲期の搜索押収の概念を詳細に検討したものとして WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT ORIGINS AND MEANING 602-1791 (2009). See also, OTIS H. STEPHENS AND RICHARD A. GLENN, UNREASONABLE SEARCHES AND SEIZURES: RIGHTS AND LIBERTIES UNDER THE LAW 19-61 (2006). 一四八五年以前には不当な搜索押収の概念はなく、一五八〇年から一六四二年の間に修正第四条の原型となる一定の不合理な搜索押収のパターンが、漠然とではあるが形成されたとする。Id. at 25, 41. 修正第四条の原理の歴史的生成について、Akil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994); William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 396-411 (1995). 連邦の司法警察権の発動はまれであったから、最初の世紀は、修正第五条も含めて修正第四条は重要ではなかった。Id. at 419. 同論文は、なるほど両条は警察官に向けられた刑事手続の原理であるが、根源は、プライバシー (その定義は議論していない) の保護を基軸として政府活動を規制するものであると指摘する。

- (22) 修正第四条に反して収集された証拠が排除されることは、判例で確立している。Weeks v. United States, 232 U.S. 383 (1914); *Mapp v. Ohio*, 367 U.S. 643 (1961).

- (23) 最高裁は一九四七年に、民間航空委員会の民間人の海外渡航の許可に関して大統領の審査を経るとする民間航空法の規定が問題となった事案で、大統領に秘密の情報管理権を認めている。「大統領は、最高司令官そして外交に関する国家機関の

両方として、利用できる諜報機関を持ち、その報告は世界に公開されないし、されてはならないものである。裁判所が、関連する情報なしに、執行権が適切に秘密と判断した情報についてなした行為を審査し、さらに無効にすることは許されないであろう」Chicago & Southern Air Lines, Inc. v. Waberman S.S. Corp., 333 U.S. 103, 111 (1947). 大統領の秘密の情報の管理権が正当化されると、秘密が秘密を生み、政策の執行やテクノロジーの発達と諜報機関の官僚組織の相乗効果で、秘密指定権の裁量が増大し、安全保障上の情報の暴露とった修正第一条の行使に影響してしまう。Heidi Kitrosser, *Classified Information Leaks and Free Speech*, 2008 U. Ill. L. Rev. 881, 887-890.

- (24) 「アメリカの諜報共同体（IC）は議会の第一級の調査に至る多くの事件やスキャンダルを経験してきている。こうした調査は、多くの場合、既存の認められてきたICの行動を明確にしたり、あるいは新たな制約を課す法律や執行命令に帰結する勧告を出している」William J. Lehmann, *U.S. Intelligence prior to 9/11 and Obstacles to Reform*, in BRUNEAU AND BORAZ, *supra* note 11 at 73, 73.

- (25) Jonathan W. Gannon, *From Executive Order to Judicial Approval: Tracing the History of Surveillance of U.S. Persons Abroad in Light of Recent Terrorism Investigations*, 6 J. NAT'L SEC. L. & POL'Y 59, 69-70 (2012). 二〇〇八年改正前までは、議会の監視はあったものの、海外のアメリカ人の電子的監視は執行権の裁量の範囲内にあった。Id. at 80.

- (26) Christopher Slobogin, *Surveillance and the Constitution*, 55 WAYNE L. REV. 1105, 1109 (2009). 後にみるように、非公開の外国諜報監視裁判所（Foreign Intelligence Surveillance Court (FISCI)）の許可に基づいて行われるが、令状を要しない場合もある。二〇〇七年、アメリカ保護法によって国家諜報長官（DNI）と法務長官が、監視が明らかにアメリカ国外にいる者に対するものと合理的に認められ、かつ外国の諜報が監視の相当な（significant）目的であるなら、令状は不要とされた。Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007). この点は後述（五）する。

- (27) Philip A. Lacovara, *Presidential Power to Gather Intelligence: The Tension between Article II and Amendment IV*, 40 L. & CONTEMP. PROBS. 106 (1976). 日本国憲法三五条と修正第四条を比較検討したものとして、中山代志子「行政調査における令状主義の適用範囲（一）（2・完）——刑事法および米国憲法修正4条からみた行政手続に関する一考察」早稲田大学大学院法研究集一四八号一二三頁、一四九号一二五頁、二〇一三年、二〇一四年。

- (28) Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 73 GEO. WASH. L. REV. 1306, 1310 (2004).

- (29) 修正第四条違反で収集された証拠能力を否定する主張の適格は、被告のうちでも限定される。Alderman v. United States, 394 U.S. 165 (1968).
- (30) 本稿で検討する電子的監視以外に、九・一一以降強化され修正第四条との関係で問題となっているものに、国境捜索がある。これは歴史的に議会の国際交易を規制する権限として修正第四条の例外とされてきたもので、令状は不要とされてきたが、同条の合理性の基準からのがれるわけではなく、問題となっている。CRS REPORT FOR CONGRESS, PROTECTING OUR PERIMETER: "BORDER SEARCHES" UNDER THE FOURTH AMENDMENT, May 17, 2005, at 1, 6.
- (31) 本人が了解してプロバイダーなどの第三者にプライバシーを提供しているから、もはやプライバシーとして保護されない。第三者理論 (Third-Party doctrine) と呼ばれる。See, Greg Nojeim and Orin Kerr, *The Data Question: Third-Party Information*, in PATRIOTS DEBATE 73 (American Bar Association, 2012).
- (32) Slobogin, *supra* note 26 at 1119.
- (33) 「民主主義社会が直面するより悩ましいジレンマの中に、その領土と制度を保全することと、同時に真に自由な個人の結合体としてそれに不可欠な自由の核を傷つけずに保全することの、それがある」。United States v. Butenko, 494 F.2d 593, 596 (1974). 外国政府にアメリカの国防情報を流した conspiracy (陰謀) の刑事事件で、政府が電子的監視を行ったことによる情報の開示を認めなかったものである。
- (34) Jack Goldsmith, *The Cyberthread, Government Network Operations, and the Fourth Amendment*, Government Studies at Brookings, Dec. 8, 2010, at 11. FISC はこれを認めざる統制の必要性を訴えている。
- (35) NORMAN ABRAMS, ANTI-TERRORISM AND CRIMINAL ENFORCEMENT 160 (4th ed. 2012). 「テロ関連の電子的監視のための司法の承認は、伝統的な捜索令状の根源と、そうした先見的な FBI の捜査の間どこかに横たわっているものとしてみられる」。Id.
- (36) 緊急事態の不安定な時代にあつては、暴力の専門集団が社会で力を持つようになってくることの警告は、肝に銘じるべきである。Harold D. Lasswell, *The Garrison State*, 46 AM. J. SOC. NO. 4, 455, at 455, 459 (Jan. 1941).
- (37) CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 3 (2007).
- (38) Id. at 8-9. これには、特定の人に絞った (target-driven) 取引監視と、特定の情報や状況に絞った (event-driven) 取引

監視がある。 *Id.* at 9, 12-13.

- (39) 修正第四条に関する重要な判例は、政府官吏が私的な文書を検索したり、私的書類の提出を命じたり、電話の会話を盗聴を行ったりしたことにかかわる。 *Stuntz, supra* note 21 at 394.

- (40) *CUDDEHY, supra* note 21 at 772. 当時、不当な搜索押収の概念が今日のように複雑になることは予想していなかったであり、不合理な搜索押収は多様で、かつ同定できる (identifiable) ものであったとする。

- (41) *Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 *MICH. L. REV.* 801 (2003). 彼は、盗聴の歴史を四つの時期に分け、第一期をこの禁酒法の時代としている (第二期は連邦交信法 (Federal Communication Act) が制定された一九三四年から一九六七年 (Katz 判決)、第三期は六七―六八年のカッツ判決時代と連邦盗聴法 (Federal Wiretap Act) 制定、第四期はそれ以降、つまりタイトル・スリーの時代)。それ以前は、修正第四条が問題となったケースは、少なくとも公刊の判例にはないとする。 *Id.* at 840-41. *Kerr* は、新たな通信技術の発達にプライバシーを保護させていくのは、裁判所ではなく立法であると指摘する。修正第四条は古典的な財産権保護の域を出ておらず、能力的にも裁判所は新たな技術の展開に憲法のみで対応していくのは困難だともいう。

- (42) *Olmstead v. United States*, 277 U.S. 438, 465 (1928) (Taff. Chief J.). 五対四の僅差の合憲判決である。法廷意見は、修正第四条の意味の拡大を否定した一方で、議会が連邦刑事司法上傍受された交信の証拠能力を制限する立法をなすのは妨げなことではない。 *Id.* at 466.

- (43) *Id.* at 471-485 (Brandeis, J. dissenting). つれに ^{ホームズ} Holmes 判事が一部同調している。 *Id.* at 469.

- (44) *Id.* at 479. 盗聴を認めるワシントン州法は刑事法違反であり、そうした手法を政府がとる、つまり公のお金で悪いことをする刑事司法は、いかなるものかとする。 *Id.* at 479-80.

- (45) *Id.* at 473. ブランドアイスはこう警告する。「自由に対する最大の危険は、熱意を持った善意の、しかし理解のない人によって、じわじわと浸食してくることにある」。 *Id.* at 479. ブランドアイスのプライバシー権の背景について、宮下紘「ルイス・ブランドアイスのプライバシー権―三四歳と三七歳のブランドアイスをつなぐ言葉」駿河台法学二六巻一頁七一頁、二〇一二年、参照。ストーン判事も反対意見を書いているが、彼は FBI 長官フーバーの元上司である。ティム・ワーナー／山田侑幸訳『FBI 秘録 上』(文藝春秋、二〇一四年) 一一八頁。

- (46) 反対意見のブライト判事はブランドイスと同じ考えだが、ホームズはこの点は慎重になっていたようである。ブランドイスがプライバシーをすでに説いていたことは知られるが、次のような認識を背景に持っていた。「進展する文明化に付随して生活が複雑で密度が濃くなっていくことは、世界から何らかの撤退を余儀なくされ、人は文化の影響を限定していく中で公表にはより敏感になっていき⁶であるがゆえに孤独とプライバシーは、個人により不可欠となった」。Samuel D. Warren & Louis O. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).
- (47) Steven C. Douse, Note, *Concept of Privacy and the Fourth Amendment*, 6 U. MICH. J.L. FORUM 154, 163 (1972).
- (48) Johnson v. United States, 333 U.S. 10, 13-14 (1948) (Jackson, J., delivering).
- (49) 個人の受話器で話されるのをそのまま聞いた電話の会話の暴露は、法 (8 605) に違反せず、なぜなら、その場合は「communication (交信)」にも「interception (傍受)」にも当たらないからだとした。Goldman v. United States, 316 U.S. 129 (1942). 壁に一方的に取り付けられた傍受装置を使用した捜査は、trespass (侵害) にあたるから無効であるとしたけれども、その内容を暴露したからといって、8 605 違反にはならないとした。Silverman v. United States, 316 U.S. 505 (1961).
- (50) 47 U.S.C. § 605 (a) (2000).
- (51) Nardone v. United States, 302 U.S. 379 (1934).
- (52) DAVID S. KRIS AND J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 3.2, West Law Next Database updated June 2013. 一九四二年、最高裁は Olmstead の判例変更を拒否しつつある。Goldman v. United States, 316 U.S. 129 (1942). 隣接するオフィスの会話を聞くため壁に盗聴装置を仕掛けることは、いかなる物理的侵入 (physical trespass) もないから合法だとした。ただし、Murphy, Stone, Frankfurter 判事は判例変更を主張した。Id. at 136.
- (53) 修正第四条でプライバシーが議論される局面は、保護される実体的権利は何かと、そうした肯定的権利を否定しようとする行為は何か⁷の二つに整理される。Douse, *supra* note 47 at 156-57.
- (54) Katz v. United States, 389 U.S. 347 (1967). 修正第四条の基本的な教義を明らかにしている。それは、「判事あるいは司法官の事前の同意なく、司法過程の外でなされた捜索は、それ自体修正第四条の下で不合理であり、特別に確立された十分に明確なくわすかな例外にのみ服する」との原理である。Id. at 357.
- (55) Id. at 353 (Stewart, J., delivering). トレスパス・ドクトリンは、もはや本条の解釈では支配的たりえないとした。「電子的

に被告の言葉を聞いたり記録したりする政府の活動（無令状の電話盗聴―筆者）は、彼が電話ボックス（telephone booth）を使用している間、正当に依拠した（justifiably relied）プライバシーに反し、したがって、修正第四条の意味での「搜索押収」に当てはまる。この目的を達成するために用いられた電子的装置が電話ボックスの壁をたまたま貫いていなかったという事実は、憲法上何の意味も持ちえない」。 *Id.*

- (56) *Id.* at 360-61 (Harlan, J., concurring). ハーランは、敷衍してこう説示する。このルールは二重（twohold）である。一つは、人がプライバシーの現実の期待を表明したこと（exhibit）、もう一つは、かかる期待に社会が合理的と認識する用意があることである。 *Id.* at 361.

- (57) *Id.* at 351-2.

- (58) *Warden v. Hayden*, 387 U.S. 294, 305-7 (1967). 「われわれは、修正第四条の主たる目的が財産よりもむしろプライバシーの保護にあると認め、財産概念に依拠した見かけの手続的な制約を次第に廃棄している。∴財産からプライバシーへの強調のこのシフトは、実体的及び手続的変革の敏感な相互作用によってもたらされた」。 *Id.* at 304.

- (59) *Sodal v. Cook County*, 506 U.S. 56, 61 (1992).

- (60) *Silverman v. United States*, 316 U.S. 505 (1961).

- (61) 389 U.S., at 357, 361 (Harlan, J., concurring).

- (62) *Id.* at 373.

- (63) *Id.* at 350-51.

- (64) 389 U.S., at 358.

- (65) *Id.* n.23.

- (66) *Id.* at 363-64 (White, J., concurring).

- (67) *Id.* at 359-60 (Douglas, J., concurring, joined by Brennan, J.).

- (68) *Id.* at 357. カットと同年の別の判例では、公的利益が私人の利益を凌駕する場合は、修正第四条の令状と相当の理由の条項の「特別に確立された例外」が認められると述べている。 *Camara v. Municipal Court*, 387 U.S. 523, 539-540 (1967).

- (69) *Attan G. Theoharis and Elizabeth Meyer, The "National Security" Justification for Electronic Eavesdropping: An Elusive*

Exception, 14 WAYNE L. REV. 749 (1968). 一九四〇年代を境に、外国の諜報、つまり安全保障のための電子的監視の執行権による慣行が積み重ねられるようになった（それ以前の電子的監視はもっぱら国内の刑事司法）歴史や実務を重視すべきとする。 *Id.* at 756.

- (70) 「有線もしくは無線で伝達される道具によって伝達された通話、送信、受信あるいはサインの情報を記録もしくは解読する装置またはプロセス」で、「ただし、いかなる会話の内容もそうした情報に含まれてはならない」。18 U.S.C. § 3127 (3).

- (71) 「最初の番号あるいはその他の通話や送信、信号化の情報を同定する受信の電子その他の電波 (impulse) を捕捉する装置またはプロセス」で、「ただし、そうした情報はいかなる会話の内容も含まないものとする」。18 U.S.C. § 3127 (4).

- (72) KRIS AND WILSON, *supra* note 52 at § 3.5. *See also, id.* n.10.

- (73) このことはすでにブランドイスらの古典的な論文が示唆していた。いわく、「近時の発明とビジネスの手法は、個人の保護と個人の保全のために、クーリー判事のいう「ひとりにしておいてもらおう」権利を斟酌される次なる段階に注意を引くこととなる。即時の写真や新聞業界は、プライバシー的な生活を浸食してしまった。そして多くの機械装置は、「クロゼットの中でちややいたことは屋根から漏れていくのである」との予言をよしとするように脅かしている」。Warren and Brandeis, *supra* note 46 at 195.

- (74) *Kyllo v. United States*, 533 U.S. 27, 32 n.1 (2001).

- (75) Slobogin, *supra* note 26 at 1120. 制憲者は「一般的な令状」による搜索を懸念した。 *Id.* at 1121.

- (76) 389 U.S. at 358 n.23.

- (77) AMERICO R. CINQUEGRANA, THE WALL (AND WIRES) HAVE EARS: THE BACKGROUND AND FIRST TEN YEARS OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, 801 (1989). つづいた議会の委議的な (deferential) 態度が、司法の審査なく執行権に電子的監視を行わせ、この分野を占領させてしまっていた。 *Id.* *See also, id.* n.40. 次に見る一九七二年の *Keith* 判決の時点でも、国内の安全保障の領域での電子的監視について、いかなる行為も議会はとることがなかった。 *Id.* at 803.

- (78) *United States v. United States District Courts*, 407 U.S. 297 (1972). 一方当事者がミシガン州の連邦地裁判事 *Keith* であつたことから、*Keith* 事件ともいわれる。法廷意見を書いた Powell 最高裁判事は、冒頭でこう述べている。「われわれの面前にある論点は、われわれ人民と彼らの政府にとって重要である。事前の司法の承認なく安全保障に関して国内の電子的監視

が授権され、法務長官を介して行動する、大統領の権限というデリケートな問題を含んでいる。これまで大統領は、議会からの指針あるいは本法院の決定的な判例なく、そうした権限を認めてきた。本件は最初にこの問題を持ち込んだ。その解決は国家的関心事項であり、違法な政府転覆や攻撃から自らを防衛する政府の権利と、不当な政府の侵入に対するプライバシーを保全する市民の権利の両方にセンシティブが要求された」。 *Id.* at 299.

(79) Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510–2520.

(80) Trevor W. Morrison, *The Story of United States v. United States District Court (Keith): The Surveillance Power*, in *PRESIDENTIAL POWER STORIES* 287, 290 (Christopher H. Schroeder and Curtis A. Bradley, eds., 2009).

(81) PETER M. SHANE AND HAROLD H. BRUFF, *THE LAW OF PRESIDENTIAL POWERS* 488 (1988). そのメモいわく、「FBIがわれわれの国益に最も伝導的なやり方でマイクロホンをカバーするのは認められるとするのが、法務省の解釈であると考ええる。FBIがその重要な諜報の任務を果たすために、国内の安全保障と国益を考量することは至上である (paramount)。したがって、国益においてこの技術を使う無制限の強制力がある」。 *Id.*

(82) カッツがオープンにさせた問題は、「司法官憲による事前の授権以外の防御が、国家安全保障を含む状況で修正第四条を満足させるか」である。 389 U.S., at 358 n.23.

(83) *New York Times Co. v. United States*, 403 U.S. 713, 728 (Stewart, J., concurring).

(84) 「情報に関する秘密は」大統領の外交権の適切な行使に高度に不可欠であるとする。 *United States v. Curtis-Wright Corp.*, 299 U.S. 304, 320 (1936).

(85) 407 U.S., at 321. 「いくつかの付加的な負担が法務長官に課せられようが、そうした不便さは憲法価値を守る自由な社会では正当化される」。 *Id.* 一方でこうも述べている。「政府たるものの最も基本的な機能は、個人とその財産の保全を提供することだとはよくいわれてきた。そして、政府が機能し人民の保全を維持させる自身の能力を防御しなければ、社会そのものは非常な無秩序となり、すべての権利も自由も危険にさらされることであろう」。 *Id.* at 312.

(86) *Powell* は保守的で、盗聴にも好意的であり、レーキストとともにニクソン大統領によって最高裁判事に任命されたばかりであったが、上院の任命の公聴会では安全保障と盗聴の問題は明確にしていなかった。 Tracey Maclin, *The Bush*

Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons from Justice

- Powell and the Keith Case*, 41 U.C. DAVIS L. REV. 1259, 1278 (2008). もっとも、政府の犯罪捜査には信頼を置いており、キース事件で上告の準備中であつた訴訟当事者にあつて、パウエルの最高最判事就任は政府にとつては良いニュースで、キース判事側にとつては悪いニュースとなつた。Morrison, *supra* note 80 at 305.
- (87) *United States v. Sinclair*, 321 F.Supp. 1074 (E.D. Mich. 1971). キースは外国の諜報と国内のそれをわけ、「完全な国内の情況にあつては、修正第四条の令状の要請から安全保障が免れる」とはなし」とした。 *Id.* at 1079-1080.
- (88) *United States v. United States District Court*, 444 F.2d 651 (6th Cir. 1971). キース判事と同じ考えで政府の主張を退けている。「政府は、大統領、法務長官、あるいは連邦法執行官を本件において修正第四条の制約から免除させる成文法の文言を、アメリカの憲法にも制定法にも判例にも何一つ示していないし、われわれも見出せない」。 *Id.* at 665.
- (89) 407 U.S., at 303.
- (90) *Id.* at 309 n.8.
- (91) PETER M. SHANE AND HAROLD H. BRUFF, SEPARATION OF POWERS: CASES AND MATERIALS 702 (3rd. ed. 2011).
- (92) 「政治的反対への危険は、政府が「国内の安全 (domestic security)」を保護する権力といった、きわめて曖昧な概念の下で行動しようとするところで、先鋭 (acute) 化する。国内の安全の利益を定義する困難が与件となつて、かかる利益を保護するために行動する濫用の危険は明白になる」。 407 U.S., at 314.
- (93) *Id.* at 308-310.
- (94) *Id.* at 313.
- (95) *Id.* at 314-15.
- (96) *Id.* at 315.
- (97) *Id.* at 316-17.^{フタラス}
- (98) *Id.* at 320. Douglas の補足意見は、国内の安全保障は修正第四条の関知するところで、修正第四条は官憲のあらゆるプライバシーへの侵入からの公的な防波堤となると強調する。 *Id.* at 321-333. ^{ホワイト}White 判事は、政府の行為は法 (82511) 違反であり、憲法問題にはならないとしている。 *Id.* at 336-37. 多数意見が当該電子的監視は違憲であると憲法レビューでとらえるのに対し、ホワイトはタイトル・スリーがこの点について規定していないから、大統領の電子的監視は違法と、制定法レビュー

ルでとらえている。

- (99) *Id.* at 318. そうした例外が認められても、「警察官は、実践可能であるならばいつでも、令状手続を通して搜索押収の司法的承認を先んじて得る」(Terry v. Ohio, 392 U.S. 1, 20 (1968))との原理を確認する。 *Id.*
- (100) *Id.* at 318-321. 「国内の安全保障の監視に適用される特別の情況は、令状主義にさらなる例外を要する。…こうした監視は一次的に転覆勢力に関する諜報の収集と維持に向けられたもので、特別の刑事訴追のための証拠収集の試みではないといわれている。このタイプの監視は、進行中の諜報情報の収集ではなく、刑事活動の捜査を支配すべく確立された伝統的な令状主義に服する要のないものであるということだ」。 *Id.* at 318-19.
- (101) *Id.* at 320. 安全保障案件は司法的評価には繊細かつ複雑すぎて手に余るとの政府の主張も認めている。 *Id.*
- (102) *Id.* at 321-324.
- (103) *Id.* at 322-23.
- (104) ROBERT M. PALITTO AND WILLIAM G. WEAVER, PRESIDENTIAL SECRECY AND THE LAW 165 (2005). 彼は辞任の一年前、「国内の安全保障事案では、大統領は初めに搜索令状をとる」となく、盗聴を授權する権限がある」と主張している。 *Id.*
- (105) *Id.* もっとも、FDRからニクソンまでの歴代大統領で比較してみると、電話盗聴の合計が七百、その年平均一二二で最低で、最大のトルーマンがそれぞれ、二七二四、三六三三であったのと比べてみても、極小といえる。 *Id.* at Table 51.
- (106) United States v. Trung Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980). アメリカ政府の極秘情報をベトナム社会主義共和国に送ったとして、スパイ行為 (espionage) とその教唆に問われた刑事事件で、いくつもの証拠が無令状での搜索押収に基づくとして、問題となった。カーター大統領と法務長官の命令でかかる捜査が行われたのである。原審は、執行権は捜査が主に (primarily) 外国の諜報の捜査であるかぎり、無令状で行えると判断していた。 *Id.* 第四控訴裁判所がこれを支持した。この問題について最高裁の判断はないが、同審はキースを類推するとした。 *Id.* 捜査の主目的が外国の諜報であるかのテストを設けている。したがって、刑事訴追の目的となった時点で無令状捜査の証拠は採用されないとした。なお、この事件はFISAが制定 (一九七八年) される前のものであることに注意したい。
- (107) *Id.* at 913-4.
- (108) 「大統領のこの領域での憲法上の特権」から、また権力分立上外国諜報監視は外交権を有する大統領の主たる責務であるこ

とから、帰結される。*Id.* at 912, 914. 下の「令状要請の外国諜報への例外」は「外国権力、そのエージェントもしくは協働者」がかかわる事例にのみ適用されたとした。*Id.* at 912, 915.

- (109) 407 U.S. at 322. これは近時の最高裁判例でも確認されている。いわく、「なるほど、キース判決は外国権力の活動に関する大統領の監視権限の射程についてのいかなる判断も明白に関わらないとしたけれども、それは暗黙に、外国諜報の監視の特別な枠組みは憲法上許容されることを示唆する」。*Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1143 (2013). キース判決を引用している。

- (110) *United States v. Brown*, 484 F.2d 418, 425-26 (5th Cir. 1973). キースは、国内の安全保障には大統領は令状を要するとしなければ、これまで下級審が判示してきたように、外交の文脈での安全保障では、大統領には憲法上の義務があるとした。「国内での安全保障の事案で適切である大統領権への制約は、国際の領域の文脈では作り物ではない (artificial)」。 *Id.* at 426.

- (111) *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974).

- (112) *Id.* at 608. 「外交の責務における大統領の重要性は、裁判所がこの領域で大統領権限に制約を置くのを求められたとき、最高の注意を以て行動するよう要請される」。 *Id.*

- (113) *United States v. Buck*, 548 F.2d 871 (9th Cir. 1977), *cert. denied*, 434 U.S. 890 (1977). 第三控訴裁判所でも、外国の諜報の情報を得るのが主目的であるならば、無令状の電子的監視は合法であるところである。*United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974) (en banc), *cert. denied sub nom. Ivanov v. United States*, 419 U.S. 881 (1974).

- (114) *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976). D.C.控訴裁判所は、外国の諜報監視を含むすべての執行権による監視にはタイトル・スリーを適用するのが憲法の精神であり、したがって事前の令状を要するとした。本件は、アメリカ国内のソ連の施設に対して暴力活動の疑いのあるユダヤ人防衛連盟に、FBIが無令状で電子的監視をなしたことへの損害賠償事件で、外国権力の諜報情報収集での電子的監視事案ではない。「緊急事態でない限り、無令状の全ての電子的監視は不合理であって、したがって違憲である」。516 F.2d, at 614.

- (115) *National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665-66 (1989). 政府の特別の必要を認め、通常の令状と相当の理由の要請から逸脱するのは正当化されるとした。

- (116) *Id.* at 675 n.3. ある下級審の判断 (United States v. Edwards, 498 F.2d 496, 500 (2d Cir. 1974)) を引用している。「危険が大型航空機を乗っ取るあるいは吹っ飛ばすのに固有の何百もの生命と何百万ドルもの財産に及ぶとき、その危険はそれだけで合理性のテストを満たす」。
- (117) アメリカの諜報は建国時にさかのぼるが、隠密に外国の諜報を行うようになったのは、FDRにはじまる。それは大統領の権限として、FBIなどの諜報機関に無令状で行わせるものであった。富井幸雄「FBIの安全保障請求状 (National Security Letters)」法学会雑誌五五巻一号三七頁、五〇―五三頁、二〇一四年。
- (118) Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007). その基本認識は「政府の情報収集を規制する重要な役割を果たすのに、修正第一条には教義的、歴史的、そして規範的な基盤が存在する」ことである。*Id.* at 116. 修正第四条や第五条で救えない部分が修正第一条の問題となり、これらはともに憲法的刑事訴訟の基盤を形成するとする。
- (119) 407 U.S. at 313-14.
- (120) キース判決の憲法的インプリケーションはいまだ健在で、国内の監視のレヴェルに限定されているものの、「無令状の電子監視という一般的トピックで、今なお最高裁の最も重要な言明である」。Morrison, *supra* note 80 at 325.
- (121) SHANE AND BRUFF, *supra* note 91 at 736-737. See also, CINQUEGRANA, *supra* note 77 at 806.
- (122) David Everett Colcon, *Speaking Truth to Power: Intelligence Oversight in an Imperfect World*, 137 U. PA. L. REV. 571, 587 (1988). もっとも「一般的には憲法が列挙する議会の権限規定から執行権の広い監視権が導き出される。*Id.* at 590.
- (123) 南米の国家への秘密裏の軍事支援や、国内に関しては共産主義者から始まって反政府的な人物や公民権運動家などへの諜報が暴露される。
- (124) 50 U.S.C. § 1801 et seq. (1982). 同法について、邦文の文献があるのでここでは詳細は触れない。岡本篤尚『九・一一の衝撃とアメリカの「対テロ戦争」法制』（法律文化社、二〇〇九年）。FISAの愛国者法による改正について、同書第五章で詳細に検討している。なお、FISAとその前後の外国諜報活動法の歴史について、See, Swire, *supra* note 28 ; SHANE AND BRUFF, *supra* note 91 at 702-708. つづいてこれらにも依拠しながら、FISAのポイントのみ触れておく。
- (125) PALITTO AND WEAVER, *supra* note 104 at 170.

- (126) SHANE AND BRUFF, *supra* note 81 at 499.
- (127) CINQUEGRANA, *supra* note 77 at 793, 794. FISAは「立法府と執行府の間の厳しい戦いの妥協であった」。Diane Caraway Plette and Jesselyn Radack, *Piercing the "Historical Mists": The People and Events behind the Passage of FISA and the Creation of the "Wall"*, 17 STAN. L. & POLY. REV. 437, 441 (2006).
- (128) 必要適切条項（二条八節一八項）によって大統領の外交権を制限できるけれども、大統領の外交目的は妨げてはならないとの説 (Prakash and Ramsey) もある。上院の司法委員会は、「本法は、司法長官が同意するように、以下の理解に基づく。なるほど、大統領は外国の諜報の目的で無令状の監視を授權する固有の憲法上の権限を有している。だとしても、議会は、外国の諜報の監視を支配する合理的な令状の手続を立法化することによって、この権限の行使を規制する権限を有する」とする。SHANE AND BRUFF, *supra* note 91 at 702. 大統領の固有の権限を制限するもので、判例にも逆行するとして、FISAそのものを違憲とする者がある。Robert F. Turner, *First Principles: Are Judicial and Legislative Oversight of NSA Constitutional?* 14 ENGAGE 84 (2003).
- (129) SHANE AND BRUFF, *supra* note 81 at 501.
- (130) 執行権のブラックパンサーの電子的監視について、スカリアDC控訴裁判所判事（当時。現在最高裁判事）は、この集団が外国の革命家とコンタクトを取っているのは広く知られており、タイトル・スリーの例外となる安全保障上の正当化事由をはきり提供していると、広くとらえている。Elisburg v. Mitchell, 807 F.2d 204, 207 (D.C. Cir. 1986). FISA制定前の事案であるが、その後の司法実務に影響をもたらしている。PALITTO AND WEAVER, *supra* note 104 at 188.
- (131) 50 U.S.C. §§ 1881b (a), 1881c (a). FISAでは、アメリカ人とはアメリカ市民と永住者はもちろん、法人化されていない (unincorporated) 相当数のアメリカ人からなる結社 (associations) も含まれる。50 U.S.C. § 1801 (i).
- (132) 50 U.S.C. § 1802 (a) (1) (2) (3) (4).
- (133) 50 U.S.C. § 1802 (b), § 1804 (a).
- (134) 法務長官の判断以外に以下の三つが、FISCTの許可なく電子的監視および物理的搜索が認められる。第一はFISCTが許可する七十二時間前の緊急の監視搜索 (50 U.S.C. § 1805 (f), § 1824 (e))。第二は電子的監視に関してのみでテストや訓練 (50 U.S.C. § 1805 (g))。第三は議会が宣戦してから一五日間 (50 U.S.C. § 1811 (電子的監視について大統領が授權))、50

U.S.C. § 1829 (身体検査))。

- (132) 50 U.S.C. §§ 1804-1805, 50 U.S.C. §§ 1823-1824.
- (136) PALLITTO AND WEAVER, *supra* note 104 at 174-75.
- (137) Pub. L. 103-359, Title VIII, § 807 (a) (3), 108 Stat. 3444 (1994), 50 U.S.C. § 1821 (5) (2012). つれにも最小限化手続 (minimization procedure) が要求される。 § 1821 (4).
- (138) 50 U.S.C. § 1861 (b) (2) (A).
- (139) 50 U.S.C.A. § 1801 (b) (1), § 1805 (a) (4). 最小限化手続は、通例、特定の通信が収集され、利用され、共有される情況に基準を提供するもので、合憲性担保や統制の機能を果たす。FISA は以下のように定義している。「法務長官によって採択される特別の手続であり、特定の監視の目的と技術に関して、外国の諜報情報を獲得し、生産し、流布させるアメリカの必要性に合致し、同意していないアメリカ人には公には利用できない情報の取得と保持を最小限にし、その流布を禁じるよう、合理的に企図されたもの」。50 U.S.C.A. § 1801 (b) (1) (2012).
- (140) 50 U.S.C.A. § 1804 (a) (7) (B)-(C), § 1805 (a) (5). アメリカ市民がターゲットになるのは、彼(女)が何らかのアメリカ刑事法の事犯になつてゐる場合である。David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 492 (2006).
- (141) 議会にとって当初からの難題は、安全保障目的の電子的監視の要請を承認するのに連邦司法判事を介在させることが可能かというものであった。かかる事案は事件争訟性を満たし、個人のプライバシーの侵害に司法の監視を置くのは司法権の根本的意図になつてゐることから、肯定された。CINQUEGRANA, *supra* note 77 at 808.
- (142) FISCt と同控訴裁判所 (FISCR) は Article III (憲法三条) 裁判所、つまり司法裁判所であるが、その判事は上院の同意に基づいて大統領が任じるのではなく、現在の任命方法には改正の動きも出つてゐる。VIVIAN S. CHU, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (FISC): SELECTION OF JUDGES, CONGRESSIONAL RESEARCH SERVICE, May 7, 2014, R43534.
- (143) FISCt の判事は政府の情報^の正確さのみを審査し、監視や政府のスパイ・プログラムの適切さを審査して判断する道具が不足していると、その首席判事 Reggie B. Walton は述べてゐる。Carol D. Leaning, *Court: Ability to police U.S.*

題視する権限を持たないなら、この判断は疑問で、本判決は執行権に過度な権限を認めることになり、プライバシーのみならず権力分立上も問題だとする。Note, *Constitutional Law-Fourth Amendment-Foreign Intelligence Surveillance Court of Review Holds that Prosecutors May Spy on American Agents of Foreign Powers without a Warrant*, 116 HARV. L. REV. 2246, 2253 (2003).

(152) 310 F.3d at 741, 745-46.

(153) *Id.* at 727. FISAの立法経緯を検証している。委員会の報告は曖昧であるが、本会議の討論 (floor debate) は明確で、FISA法案は法執行と諜報の伝統的なバリアを壊したのであり、それは国際テロとの戦いのためというよりも、外国諜報の広範な定義に刑事捜査がオーバーラップするためだとの議論に注目している。

(154) Turner, *supra* note 128 at 84.

(155) William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma—A History*, 11 LEWIS & CLARK L. REV. 1099, 1106 (2007).

(156) Weeks v. United States, 232 U.S. 383 (1914). については私有財産の保護が修正第四条の核とされたが、それは、こうした違法な財産剥奪に対する救済に利用できる面があったからとみえる。Warden v. Hayden, 387 U.S. 294, 304 (1966).

(157) 主要な目的テストとされる。「監視は刑事捜査が主であるとなれば、裁判所は通常の相当な理由 (probable cause) の決定をなすのに完全な権限を有するのであり、なぜならば、重要なことに、政府が刑事訴追のための基盤を主に形作るうとしているとき、個人のプライバシーの利益が前面に出てきて、政府の外交政策の関心は後退するからである」。629 F.2d at 915.

(158) Kris, *supra* note 140 at 487-8, 499.

(159) <http://www.fas.org/irp/agency/doj/fisa/1995procs.html> の背景や制定過程について、Piette and Radack, *supra* note 127 at 467-478; Kris, *supra* note 140 at 499-506. 一九九四年のAldrich Ames事件 (CIA防諜部員が一九八五年からスパイ活動をしていた) でのFBIや法務省内での法執行・司法警察部門と安全保障諜報部門との度を越えた交流への反省が大きい。

(160) Piette and Radack, *supra* note 127 at 478. Kris, *supra* note 140 at 499. Krisは壁の歴史を七つの時期に分けて、詳細に分析している。 *Id.* at 499-518. 本節の以下の記述はこれに大きく依拠している。

- (161) 「壁は、一九九五年に法務省によって採択された手続に基づいて、連邦法執行官吏と諜報官吏がお互いに情報を調整し、助言し、共有することができないことの比喩である」。Cedric Logan, *The FISA Wall and Federal Investigation*, 4 N.Y.U. J.L. & Lib. 209, 222 (2009). ついに主要な目的テストが成文化された。 *Id.* at 229.
- (162) 50 U.S.C. §§ 1806 (k) (1), 1825 (k) (1).
- (163) 310 F.3d. at 733-34. 「外国の諜報の情報を得るべく、FISAの監視を立ち上げ、実施し、継続し、あるいは拡大させることについて、FBIの諜報部に助言する刑事検察官の能力を、たとえそうした情報が外国の諜報の犯罪の証拠を含むとしても、制限される」との解釈には、「いかなる根拠もない (no basis)」。 *Id.* But see, Funk, *supra* note 155 at 1123. いわく、FISAの立法経緯や趣意は、FISAが決してタイトル・スリーにとって替わるものであってはならない明白なメッセージを出している。
- (164) 必要な免許なく中国に軍事技術を提供したことが輸出統制法に反するとされた刑事事件で、この情報がFISAに基づいて収集されたにもかかわらず、刑事事件に証拠として使用されたことが、「主要な目的」要件の修正第四条に反しないかが争われた。 *United States v. Ning Wen*, 477 F.3d 896 (7th Cir. 2007). FISAは「相当な理由」としており、FISCは外国の機関が法律に違反しているかの相当な理由を判断する必要はない。修正第四条は排除ルールにはよき根拠たりえないとし、相当な理由のある外国機関との傍受で取得された国内犯罪の証拠は、国内の事犯について知ることが期待されるか否かにかかわらず、国内の刑事訴訟に使用されうとした。 *See also*, *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984).
- (165) 310 F.3d. at 723, 731, 736. 証拠収集が可能な犯罪はFISAの § 1801 (a)-(e) で言及されているとする。
- (166) 「壁それ自体は搜索監視活動への決定的な制約ではない。むしろ、法執行官吏を諜報捜査から離しておくことで政府が履行する順応性のある (malleable) 要件である」。Kris, *supra* note 140 at 518.
- (167) *Id.* at 520. But see, Funk, *supra* note 155 at 1136-1139. Funkは、壁は主要目的を掲げるFISAのもともとの趣旨であり、政府がFISAで取得しようとすることに横たわる諜報／法執行の二分法 (dichotomy) には長い伝統があり、FISAはこれを単純に踏襲しようとしたものである。壁の消去あるいは変更は、刑事司法の証拠収集に広範な侵害的捜査手法を認めることになっていると批判する。
- (168) 「壁を再建すれば、われわれ自身の安全保障機関が起こし得る濫用と外国の脅威からアメリカ人を安全にさせなくなる」。

Kris, *supra* note 140 at 529. *But see*, Logan, *supra* note 161 at 250. 裁判所も法務省も、壁あるいは主要な目的テストが憲法上の要請とみづいたと分析している。

- (169) PALLITTO AND WEAVER, *supra* note 104 at 185.
- (170) Smith v. Maryland, 442 U.S. 735 (1979).
- (171) *Id.* at 742–744. 「電話使用者は典型的に電話会社に番号情報を伝えなければならないことを知っており、電話会社はこの情報を記録する設備を持っており、電話会社は事実、多様な正当のビジネス目的でこの情報を記録しているのである」。 *Id.* at 743. これは踏襲やれつゝる。 *See, e.g.*, United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009). 「いわゆる第三者の法理であり、学説には批判も強い。肯定的に検討したのもふたつ」 Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561 (2009).
- (172) EDWARD C. LIU, ANDREW NOLAN AND RICHARD M. THOMPSON II, OVERVIEW OF CONSTITUTIONAL CHALLENGES TO NSA COLLECTION ACTIVITIES AND RECENT DEVELOPMENT, CRS R43459, Apr. 1, 2014, at 6.
- (173) 18 U.S.C. § 83121–27 (2000).
- (174) Kyllo v. U. S., 121 S. Ct. 2038 (2001) (Scalia, J., delivering).
- (175) *Id.* at 2043.
- (176) *Id.* at 2047 (Stevens, J., dissenting).
- (177) U.S. v. Jones, 132 S. Ct. 945 (2012) (Scalia, J., delivering).
- (178) *Id.* at 949. 同条は財産を保護しトレスパスにかかわるが、カッツでとられたプライバシーを判断するには及ばないとする。 *Id.* at 950. なおこの判決の邦文紹介として「[2013] アメリカ法 (356)」。
- (179) Olmstead v. United States, 277 U.S. 438, 472 (Brandeis, J., dissenting).
- (180) 533 U.S., at 29.
- (181) *Id.* at 31.
- (182) *Id.* at 34. 興味深いのは「originalism (原意主義)」、それも憲法の文言は制憲時に通常の意味で使用されていたものが意味となるこの立場の Scalia が、当時はそうした技術がなかったことで本件にはこのアプローチが適用し得ず、物理的侵入

(physical intrusion) の意味を現代的状況に翻訳している¹⁸⁷。Lawrence Rosenthal, *Originalism in Practice*, 87 IND. L.J. 1183, 1208 (2012). この論文は、originalism をもとに期待された適用と語義的原意主義に整理して、現代では非原意主義にならざるをえなくなっていると分析する。

- (183) 132 S. Ct., at 951–52. See also, Spencer S. Cady, Note, *Reconciling Privacy with Progress: Fourth Amendment Protection of E-Mail Sored with and Sent through a Third-party Internet Service Provider*, 61 DRAKE L. REV. 225, 239 (2012). ショーンズ判決で最高裁は、GPS の設定と使用は一八世紀的な意味での搜索に当たるとの類推には関係がないとしたうえで、「新たな搜索の方法がどのように工夫されようとも、われわれの仕事は最低限、問題となっている行為が修正第四条の原意内の搜索を構成したかを決定するところにある」とする。132 S. Ct., at 950 n.3.

- (184) STEPHEN BREYER, ACTIVE DUTY: INTERPRETING OUR DEMOCRATIC CONSTITUTION 66 (2005). プライバシーを、「彼または彼女について他人が知るようになりうるものをコントロールする個人の力」と定義している。

- (185) Thomas K. Clancy, *What does the Fourth Amendment Protect, Property, Privacy, or Security?* 33 WAKE FOREST L. REV. 307 (1988).

- (186) 「プライバシーの合理的な期待テストは修正第四条法の際たる¹⁸⁸ステリーである」。Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504 (2008). Kerr はこのテストに、¹⁸⁹なにが憲法上合理的であるかを示す類型として、蓋然性 (probabilistic) モデル (分別ある人が自らのプライバシーを維持するものとあらかじめ思っている機会で判断)、私的事実 (private facts) モデル (政府が集める情報に着目し、その情報が憲法上プライバシーとして保護される価値があるかで判断)、実体法モデル (政府の行為を規制する実体法があるかで判断)、政策モデル (警察の行為が令状を要するとすべきかの政策的見地から判断) の四つが存在し、混淆していると分析している。Id. at 508, 512, 516, 519.

- (187) 389 U.S., at 353.

- (188) 特別の必要性の法理については以下に基づく。Goldsmith, *supra* note 34 at 12.

- (189) *Cassidy v. Chertoff*, 471 F.3d 67 (2d. Cir. 2006). この時の判事が現最高裁判事の¹⁹⁰Sotomayor である。

- (190) In re Directives Pursuant to Section 508 of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008).

- (191) 政府がアメリカ国外に「合理的に」と信じられている」外国諜報のターゲットを監視するのに令状の要請を廃止したもので、FISA改正法(The FISA Amendments Act of 2008)はFISA第七章のアメリカ保護法の多くの規定を再授權した。この点は本稿五で検討する。
- (192) 551 F.3d, at 1011.
- (193) *Id.* at 1013. 防御のマトリックスは、ターゲットの手続、侵害を最小限にする(minimization)手続、監視の有意な目的(significant)が外国の諜報の情報にであることを確保させる手続、大統領命令(EO 12333)に編入された手続、認証の根拠となるaffidavit(宣誓供述書)で示された手続の、少なくとも五つが認められるとする。
- (194) *In re Sealed Case*, 310 F.3d 717, 745-6 (Foreign Int. Surv. Ct. Rev. 2002).
- (195) *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000).
- (196) *New Jersey v. T.L.O.*, 469 U.S. 325, 358 (1985) (Brennan, J., dissenting).
- (197) *MacWade v. Kelly*, 460 F.3d 260 (2d Cir. 2006). *See also, Criminal Law-Fourth Amendment*, 120 HARV. L. REV. 635 (2006). 同裁判所は特別の必要性の法理での衡量に四つのテストを設けた。第一に、テロリスト抑止の政府利益は差し迫った実質的なものである。第二に、地下鉄の乗客は客観的にも主観的にもプライバシーの合理的な期待を十分に享受している。第三に、地下鉄の搜索プログラムはそのプライバシーの期待に最小限の制約しかもたらさない。第四に、地下鉄のテロ攻撃を効果的に抑止するのに合理的な手法である。*Id.* at 637-38.
- (198) *Goldsmith, supra* note 34 at 14. 彼はそれ以外にも時限立法など統制の手法を提案している。*Id.* at 14-16.
- (199) *Laura K. Donohue, Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1072 (2006). 長大な論稿でアメリカとイギリスの安全保障とプライバシーの関係を法的に分析し、バランスのとれた制度への改革を提言している。
- (200) *Amar, supra* note 21 at 770-71 (1994). イングランドでは令状は執行権の裁量であることが少なくともなく、さらに制憲当時、司法官に対する不信も相当であったとする。^{アマー}*Amar*は、令状主義ではなく合理性の統制に着目(これが第一の原理ということか)すべきことを説く。それは常識の合理性ではなく、憲法上での合理性であるという。「修正第四条ははっきりと、手続的はもちろん、実体的な不公平さ(unfairness)を語っており、合理的と非合理的の政府の政策を区別する必要性を公

然と主張している」。*Id.* at 811.

(20) 前掲注(17)。

(202) Zweibon v. Mitchell, 516 F. 2d 594, 601 (1975). *See also*, Glenn Sulmasy and John Yoo, *Katz and the War on Terrorism*, 41 U.C. DAVIS L. REV. 1219, 1248 (2008). ウォーターゲート事件の後、政府の諜報活動を洗いざらい追及したチャーチ委員会 (U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities) が、「一九三〇年代以降、諜報機関は司法令状の恩恵なしにアメリカ人をしばしば盗聴してきた」として、そこには議員や政府活動家も含まれるとしている。INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATION, BOOK II, 94th CONG. 2d. Sess., REP 94-755, 1976, at 12. F.D.R. 一九四〇年のメモは、議会の制約を受けないで安全保障のための電子的監視を行う執行権の権限を宣言したものである。KRIS AND WILSON, *supra* note 52 at 83.3. 戦後、トルーマン大統領に受け継がれ、国家転覆活動の疑いのある者への傍受にまで拡大された。*Id.* その後ジョンソン大統領のときは、通信傍受を安全保障目的に限定し、かつ事前に法務長官の承認を経ることとした。この間、こうした措置が修正第四条や連邦交信法に反するとした判例はない。*Id.* at 83.4.

(203) 大統領のスト防止のための鉄鋼所国有化措置が違憲と判断された判例で、大統領の憲法上の権限の解釈について三つの類型を示した。第三類型は「大統領が議会の明示または黙示の意思に矛盾する措置を取る時、その権限は最低網 (lowest web) となり、その事項に関する議会の憲法上の権限を引いた自らの憲法上の権限のみに依拠できる」との公式である。Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-637 (1952)。これについて、富井幸雄「軍権と行政権」比較憲法学研究二一号二五頁、四〇頁、二〇〇九年、参照。

(204) Heidi Kitrosser, *It Came from beneath the Twilight Zone: Wiretapping and Article II Imperialism*, 88 TEX. L. REV. 1401 (2010). Kitrosser は排他的大統領権者ではなく、諜報での電子的監視は憲法上、議会の立法に服するとの立場から、議会や裁判所で今や優勢となっている排他的大統領権者が制憲後の運用の歴史を根拠としている議論を論難する。

(205) C & S, Air Lines v. Waterman, S. S. Corp., 333 U.S. 103, 111 (1948) (Jackson, J., delivering). 行政訴訟を認めた民事航空法 (Civil Aeronautics Act) の規定は、大統領の権限である外国の航空運輸に従事するアメリカ市民の許認可命令には適用されないとした。「裁判所は、執行権の秘密を考量するためにイン・カメラで審理することもできない。かりに裁判所が完全

- な開示を要求できたとしても、外交政策に関する執行決定の性質はまさに政治的であって、司法的ではない」。 *Id.*
- (206) 規約の順守や衛生管理の点検のために、市職員の住宅への定期的な無令状での立ち入りを認め、これを拒否した者に刑事罰を科す条例の合憲性が問題となった。 *Canara v. Municipal Court of the City and County of San Francisco*, 387 U.S. 523 (1966). 最高裁は、修正第四条が「政府の官憲による無節操な侵害から個人のプライバシーと保全を守る目的である」とし (*Id.* at 528)、「所有者の財産権そのものが保護されるところで、行政上の目的であっても修正第四条が保護した権利の重大な侵害であり、特に緊急事態でなければ、令状が必要となるとした。 *Id.* at 539 (White, J., delivering)。
- (207) *Orin S. Kerr, The Modest Role of the Warrant Clause in National Security Investigations*, 88 TEX. L. REV. 1669, 1669 (2010).
- (208) *Id.* at 1680.
- (209) これには、(a) 令状を要求するとするも、令状の要件は不明のままにしておく、(b) 既存の確立した制定法の令状制度が憲法上の手本を満たしているかを評価する、の二つのパターンがあるとする。 *Id.* at 1679–80. キースは前者である。
- (210) *Id.* at 1684.
- (211) *Maclin, supra* note 86 at 1317. したがって、政府がテロ監視プログラムには令状主義が適用されないとの主張は説得力を欠く。 *Id.* at 1318.
- (212) AUDIT OF THE DEPARTMENT OF JUSTICE'S IMPLEMENTATION OF AND COMPLIANCE WITH CERTAIN CLASSIFICATION REQUIREMENTS, U.S. DEPT. OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL 23 (2013).
- (213) JARED P. COLE, DISCLOSURE OF FISA OPINIONS-SELECTED LEGAL ISSUES, CONGRESSIONAL RESEARCH SERVICE, CRS 7–5700, R43404, Feb. 24, 2014.
- (214) 秘密指定 (confidential, secret, top secret) には執行権の裁量が認められるとはいえず、議会や裁判所がどこまで介入できるかは明確ではなう。一九七四年のFOIA (情報公開法) 改正後、裁判所は執行権に委譲する傾向が顕著となっているが、立法で始審的 (*de novo*) を可能にするのは憲法上問題なことの指摘もある。 *Note, Keeping Secrets: Congress, the Courts, and National Security Information*, 103 HARV. L. REV. 906 (1997).
- (215) *United States v. Smith*, 321 F. Supp. 424, 429 (C.D. Cal. 1971). *See also, United States v. Sinclair*, 321 F. Supp. 1074, 1080 (E.D. Mich. 1971).

- (216) William C. Banks and M. E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 19-31 (2000).
- (217) Peter E. Quint, *The Separation of Powers under Nixon: Reflections on Constitutional liberties and the Rule of Law*, 1981 DUKE L.J. 1, at 23 n.101. 海外の諜報活動についても政治目的でなされる(例えば共産主義思想の動向など)ものが少なからず海外にかけつけ国内のそれした配慮に押されてなされるのである。Note, *Foreign Security Surveillance and the Fourth Amendment*, 87 HARV. L. REV. 976, 987-88 (1974).
- (218) Sulmasy and Yoo, *supra* note 202 at 1229-1230.
- (219) Banks and Bowman, *supra* note 216 at 18.
- (220) Washington to Col. Elias Dayton, July 26, 1777, in 8 WRITINGS OF GEORGE WASHINGTON 478-9 (John C. Fitzpatrick ed. 1935).
- (221) FEDERALIST NO. 64, at 434-35 (John Jay) (Jacob E. Cooke, ed. 1961). 前掲注(17)。ジェイのこの言明は条約締結のプロセスでの執行権の秘密の特権を正当化するものであるが、広く執行権の秘密の諜報権能の正当化として引き合いに出される。Ransom, *supra* note 15 at 52-53.
- (222) Robert F. Turner, *Constitutional and International Law Implications of Executive Order 13440 Interpreting Common Article 3 of the 1949 Geneva Conventions, Prepared statement before Select Comm. on Intelligence U. S. Senate*, Sep. 25, 2007, at 13. 大統領と議会で最強の諜報機関を創設していくことで争いが生じたことはなく、主たる公的論争も生じなかったものであり、「立憲システムは諜報機能を促進させるように機能してきた」とされる。Ransom, *supra* note 15 at 68-69.
- (223) 前掲注(202)。
- (224) 「諜報収集は大統領が(効率的な防衛)を遂行しうる不可欠の道具である。憲法条文と構造から黙示されることは、安全保障の決定はしばしば、議会よりもむしろ大統領を特徴づける行動に、目的と精力の統一を必要とする実践的な考慮によって裏付けられる」。Sulmasy and Yoo, *supra* note 202 at 1237.
- (225) *Id.* at 1239, 1248. 「FISAは、執行権に令状をもらうよう裁判所に行くことを要求している点で、妥協である。それまでは、執行府 (Executive Branch) は判事から許可をもらう必要はなく、安全保障の理由で捜索を行うことができた。…

(執行権寄りのこうした考え方は)、執行権が司法権より安全保障の要請をよりよく満足させることができるから、また、大統領は安全保障の憲法上の義務を有するから、裁判所は令状なしの諜報の搜索を行う大統領の権限を制限しようとすべきではないことを認識したものである」。Id. at 1239.

- (226) 「多くの安全保障法は手続である」として電子的監視法制に言及する。JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 23 (2007).

- (227) 同法の制定経緯や論点について、富井幸雄『海外派兵と議会』（成文堂、二〇一三年）第四章、参照。

- (228) Quint, *supra* note 217 at 25. なおQuintは、ニクソンがとった執行権の行為には、自らが一般的規範を定立するものと立法なくして憲法上の人権を侵害するものの二つがあるとし、ともに違憲であって、立法の授權を要するものだとし、司法の積極性を主張する。キースは後者に位置づけられる。

- (229) FISAは安全保障とプライバシーの双方のバランスをとった立法だと評価する者として、Ira S. Shapiro, *The Foreign Intelligence Surveillance Act: Legislative Balancing of national Security and the Fourth Amendment*, 15 HARV. J. ON LEGIS. 119 (1978).

- (230) MacIn, *supra* note 86. キースを踏みにじっているとする。FISA違反の恐れもありうるが、FISAは合衆国をターゲットにしているテロリストには無令状で電子的監視を認めているから、これに当てはまるとすればよいであろう。大統領側は、FISAとの適合性は大統領の憲法上の権限であるから議論するに及ばないとしている。Id. at 1302-3.

- (231) Id. at 1293. ACLU v. NSA, 493 F.3d 644, 648 (6th Cir. 2007). TSPが修正第四条に違反しているかが争点となった。裁判所は、原告はTSPが実施されたと実証していないので原告適格を欠くとして、憲法問題には立ち入らなかつた。さらに行政手続法の行政処分 (agency action) を争ってはいないとした。なお、NSAの本件盗聴にタイトル・スリーは適用されないとし、不適用の要件を四つ挙げている。すなわち、①外国諜報活動に従事している②他に適用される連邦法があり、これに従っている③監視が外国の電信システムを含んでいる④FISAで規定された電子的監視以外の手段を使用しているである。また、本件はFISAの対象でもないとした。Id. at 681. 原審はTSPが無令状での電話盗聴であるとして、修正第一条、第四条に違反していると判断してゐた。ACLU v. NSA, 467 F. Supp. 2d 754 (E.D. Mich. 2006). なお、政府が気に入らない出版を抑圧するための制度として、搜索押収権限を使ってきた歴史がある。Marcus v. Search Warrant, 367 U.S.

717, 724 (1961). 猥褻物を取り締まるためのミズーリ州の包括的な令状を違憲としたもので、修正第十四条を通して修正第四条が適用される。

- (232) 大統領は最高司令官であって、テロとの戦争にあるのだから、こうした権限は当然認められると支持する者として、John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565 (2007). ためおしとして、AUMFで立法府も容認しているとも説く。TSPが立法からフリーだとするブッシュ43側の考えの根拠は、次の三つに整理されよう。第一にFDR以来の慣行で、大統領は立法がなくてもこれにこだわることなく盗聴を実施してきた。第二に、こうした大統領主導＝議会忍従は両部門の憲法上の権限を尊重した結果である。第三に、この議会の長期にわたる忍従は、自らが諜報収集を制約する憲法上の権限がないとの認識を反映している。こうした議論は能力を法的特権に融合させる誤った解釈で、大統領の排他的権限を正当化するものではないと批判される。Kirosser, *supra* note 204 at 141. See also, David Gray Adler, *George Bush and the Abuse of History: The Constitution and Presidential Power in Foreign Affairs*, 12 UCLA L.J. & FOR. AFF. 75 (2007). 大統領固有権論は制憲者の意思に反しており、ブッシュが制憲史からこれを説くのは誤謬だとする。*Id.* at 83, 93-94, 141.

- (233) *Id.* at 3. 国内での諜報活動は、キースとそれを受け継いだFISAに照らして、憲法は制限している以上、修正第四条に反するとし、やうにターゲットを絞り込むために行っているならなおやうだとする。William Banks, "If Men Were Angels" NSA Eavesdropping and the Fourth Amendment, 28 ABA NATL. SEC. L. REP. 1-2 (2006). But see, Robert Turner, *National Security Law and the NSA-FISA Controversy*, 28 ABA NATL. SEC. L. REP. 7-9 (2006). 判例は大統領に固有の諜報権限を認めており、修正第四条の不合理なという制約は及び、議会はこれを緩めることはできても、大統領のこの裁量を制限することはできないとする。一方、マイクロでの秘密性 (micro-secrecy) は認められるにしても、マクロの透明性 (macro-transparency) は憲法上の指令だとして、ブッシュ43はこれをつつちやにした誤った憲法解釈で秘密権限を拡大させていると批判する者もいる。Heidi Kirosser, "Macro-Transparency" as Structural Directives: A Look at the NSA Surveillance Controversy, 91 MINN. L. REV. 1163 (2007).

- (234) 407 U.S. at 303, 82511 (3) を「議会の但書と中立の表現とみれば、制定法は本件で断定された執行権の権限を計る (measure) ものではないと判断する。むしろわれわれは、大統領の憲法上の権限を見なければならぬ」。 *Id.* at 308.

- (235) BAKER, *supra* note 226 at 89–93.
- (236) *Id.* at 96–98.
- (237) *Id.* at 79.
- (238) リンカーンとのスパイ契約 (espionage) に関する損害賠償請求事件で、最高裁は、大統領は最高司令官条項 (憲法一条) でかかる契約を結びうるし、その履行は秘密裏になされることを旨としているのであり (secret service)、公表されないのは公政策であるとした。Totten v. United States, 92 U.S. 105 (1875).
- (239) Eric L. Richard, “Unlashing” the intelligence Community, 69 ABA J. 907, 910 (1983).
- (240) See, e.g., In re Sealed Case, 310 F.3d 717, 746 (Foreign Int. Surv. Ct. Rev. 2002).
- (241) その判断は、議会監視からも最高裁のレビューからも、実務的観点だとして排されており、「一人のFISCの判事と三人のFISCの判事と、大統領と法務長官によって創設されたまさに秘密の憲法であって、修正第四条の判例と、プライバシー権と、刑事訴訟と修正第一条の権利に踏みこめない秘密のベールの下に再構成する憲法である。アメリカ市民を侵害的に監視するのに従事するのは大統領の当然の権限だとの誤った信条の下で、議会が執行府の機関に移送した権力なのである」。PALITTO AND WEAVER, *supra* note 104 at 192.
- (242) Kerr, *supra* note 207. 「安全保障のセッティングでは、令状条項は控えめのままでなければならない」のであり、「詳細は立法に委ねよう」。 *Id.* at 1670, 1684.
- (243) *Id.* at 1671, 1677.
- (244) 富井、前掲(山)論文、参照。
- (245) 5 Hearings Before S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities: National Sec. Agency and Fourth Amendment Rights, 94 th Cong. 2–3 (1976).
- (246) JOHN NORTON MOORE AND ROBERT F. TURNER, EDS., NATIONAL SECURITY LAW 940 (2nd ed. 2005).
- (247) Clapper v. Amnesty Int'l, 568 U.S. —, 3 (2013) (Alito, J., delivering). ブッシュ43政権下のNSAによる電子的監視について、岡本、前掲(24)書、二一六―二三五頁、土屋、前掲(5)書、第八章「ブッシュ政権の令状なし通信傍受」、参照。
- (248) 568 U.S., at 4.

- (249) *Angela Merkel: NSA snooping claims 'extremely serious'*, THE GUARDIAN, July 3, 2013. スノーデンは二〇一三年のタリスブスを前に、一連の暴露の使命は果たしたと信じていた。Edward Snowden, *after months of NSA revelations, says his missions accomplished*, WASH. POST, Dec. 23, 2013.
- (250) 上の段落の記述は以下に基づく。Liu, NOLAN AND THOMPSON II, *supra* note 172 at 3-4.
- (251) Robert S. Litt, ODNI General Counsel, *An Overview of Intelligence Collection*, July 18, 2013, <http://icontherecord.tumblr.com/post/57724442606/last-visited>, July 24, 2014. すなわち「政府の三部門すべてはこれらのプログラムを知っており、承認し、適法になされるように支援したのである」。なお、大林啓吾「プリズムの衝撃―監視国家と立憲主義」(1)(2)(3) JCLU Newsletter 三八七号八頁、三八八号八頁、三八九号八頁、二〇一三年、参照。
- (252) スノーデンの行為を評価し諜報活動の違法な実態を糾弾するものとして、グレン・グリーンウォルド／田口俊樹・濱野大道・武藤陽生訳『暴露』(新潮社、二〇一四年)。
- (253) LIBERTY AND SECURITY IN A CHANGING WORLD : REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, Dec. 12, 2013, この研究会のメンバーは Richard Clarke, Michael Morell, Geoffrey Stone, Cass Sunstein, Peter Swire である。
- (254) MARSHALL CURTIS ERWIN AND EDWARD C. LIU, NSA SURVEILLANCE LEAKS: BACKGROUND AND ISSUES FOR CONGRESS, CRS REPORT FOR CONGRESS, July 2, 2013, CRS7-5800, www.crs.gov/R43134. 愛国者法二一五条は二〇一五年六月一日に失効することになっている。議会はアメリカ自由法 (USA Freedom Act) 案をめぐってNSAの大量データ収集のあり方を審議していたが、六月二日に上院で六七対三三づれを可決し、NSAのこの活動を終わらせようとしている。
- (255) *Obama calls for significant changes in collection of phone records of U.S. citizens*, WASH. POST, Jan. 18, 2014 ; *Obama's restrictions on NSA surveillance rely on narrow definition of 'Spying'*, WASH. POST, Jan. 18, 2014.
- (256) ホワイトハウスの二〇一三年の報告書は、NSAが収集する情報の多くはテロリストと関係のない市民のもであり、なんら違法な行為の証拠になるものではないという重要な二点を斟酌していないと批判される。Recent Administration White Paper, 127 HARV. L. REV. 1871, 1875 (2014).
- (257) 防諜 (counterintelligence) は、敵国とその諜報機関による侵入と攪乱から自国の諜報工作を防護する取り組みで、分析的

であると同時に工作的である。すなわち防衛行為以上のものであって、収集、防衛、攻撃のタイプがある。ローエントール、前掲(5)書、一八七頁。

- (258) Presidential Policy Directive/PPD-28, Signals Intelligence Activities, Jan. 17, 2014.
- (259) 本節は以下に依拠している。NSA of Hrd' <http://www.nsa.gov>; RICHELSON, *supra* note 9 at 30-36. 国家インテリジェンスの情報収集の手段は、人的情報 (human intelligence; Humint)、公開情報 (OSINT)、技術情報 (TECHINT) に分類され、TECHINTはさらに通信情報 (SIGINT) や画像情報 (IMINT) などに分類される。小谷、前掲(5)書、六七-一〇五頁。NSAに至るアメリカのSIGINTの展開について、デイヴィッド・カーン／秦郁彦・関根英夫訳『暗号作戦』(早川文庫、昭和五七年)、参照。NSAの歴史と諜報活動の中身について、ジェイムズ・バムフォード／滝沢一郎訳『パズル・パレス』(早川書房、昭和六一年)、参照。
- (260) プリズムを含む詳細なNSAの電子的監視の仕組みと実績について、See, WAYNE MADSEN, NATIONAL SECURITY AGENCY SURVEILLANCE: REFLECTIONS AND REVELATIONS, 2001-2013 (2013).
- (261) NSA goes on 60 Minutes: the Definitive facts behind CBS's flawed report, THE GUARDIAN, Dec. 16, 2013.
- (262) Rajesh De, *The NSA and Accountability in an Era of Big Data*, 7 J. NAT'L SEC. L. & POL'Y 301, 303 (2014). 「NSAは国防長官の指揮で軍事作戦を支援するとともに、DNIによって調整された国家的要請に応じて諜報の報告を作成する。Id. じられる非アメリカ人を対象にすることを、法務長官とDNIに合同に授權することを認めた。50 U.S.C. § 1881a. これは一年間効力を有するが、いくつかの制約もある。50 U.S.C. § 1881a (b). 第一に、国内にいると合理的に分かっている間には、なんびとをも意図的に標的にすることはできない。第二に、国内に合理的にいると信じられる特定の個人を標的にする目的で、国外に合理的にいると信じられる者を故意に標的にできない。第三に、国外に合理的にいると信じられるアメリカ人を故意に標的にできない。第四に、収集の時全ての情報の送受信者が国内にいるとわかっているのに、故意に交信を取得することはできない。第五に、修正第四条に符合したやり方で行われなければならない。」
- (264) Laura K. Donohue, *NSA Surveillance may be legal—but it's unconstitutional*, WASH. POST, June 21, 2013, http://articles.washingtonpost.com/2013-06-21/opinions/40110321_1_electronic-surveillance-fisa-nsa-surveillance, last vis. Nov. 25, 2013.

- (265) 50 U.S.C. § 1881a (d), (e). LIU, NOLAN AND THOMPSON II, *supra* note 172 at 11. なぞ、犯罪の証拠となる場合はアメリカ市民の情報にどうも認められる。
- (266) Walter Pincus, *The other side of the Surveillance story*, WASH. POST, Aug. 14, 2013. *See also*, Steven G. Bradbury, *NSA phone collection efforts shouldn't be constrained*, WASH. POST, July 22, 2013.
- (267) De, *supra* note 262.
- (268) *Id.*, *supra* note 251.
- (269) Stephen I. Vladeck, *Big Data before and after Snowden*, 7 J. NAT'L SEC. L. & POL'Y 333, 336 (2014). Big Data は大量であつて従来の管理方法では処理しきれず、新たな手法が必要と認識を促さる。BABAK AKHGAR, GREGORY B. SAATHOFF, HAMID ARABIA, RICHARD HILL, ANDREW STANFORTH, AND PETRA SASKIA BAYERL, APPLICATION OF BIG DATA FOR NATIONAL SECURITY 3 (2015).
- (270) In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, at 6, 9 (FISA Ct. 2013). <http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf>
- (271) Klayman v. Obama, Civil Action No. 13-0851 (RJL), Dkt.#13 (13-0851), #10 (No. 13-0881).
- (272) *Id.* at 47. ーヤーンがどうする。
- (273) *Id.* at 57-58.
- (274) NSA goes on 60 Minutes: the Definitive facts behind CBS's flawed report, THE GUARDIAN, Dec. 16, 2013.
- (275) 大量の収集に反対する旗手である諜報委員会の Ron Wyden ^{ロナン・ウェーデン} 上院議員は、NSA の収集するメタデータは「人間関係のデータベース (human relation database)」とみる。
- (276) LIU, NOLAN AND THOMPSON II, *supra* note 172 at 7-8.
- (277) Veronia School District 47J v. Acton (94 — 540), 515 U.S. 646, 653, 656-60 (1995) (Scalia, J., delivering).
- (278) American Civil Liberties Union v. James R. Clapper, 13 Civ. 3994 (WHP), USDC SDNY, Dec. 27, 2013.
- (279) *Id.* at 52. 「」の収集は広範であるが、対テロの捜査の範囲は前例がない。安全保障の捜査は刑事捜査とは根本的に異なる。

それは、刑事が適及的な捜査であるのと対照的に、攻撃を未然に防ぐことに焦点を置く将来的なものである。安全保障の捜査は長期間をスパンにとり、地理的範囲も拡散する。：議会は、明らかに広範な必要性を認識して、テロリストの脅威を抑止する道具を政府に提供したのである」。 *Id.* at 36. なお判決は五三頁もある。

- (280) Turner は、下級審で合憲判決が多く出されるようになれば、最高裁はこれにあえて口を出すことはないだろうとして、司法レビューでも NSA のこの監視の合憲が固まるとする。 Jennifer Smith and Jacob Gershan, *Judge Backs the NSA's Surveillance*, WALL ST. J., Dec. 28, 2013.

- (281) 二〇一五年五月七日、第二連邦控訴裁判所は、NSA のメタデータ収集は、愛国者法二一五条に反しているとして、ニューヨーク地裁に審理を差し戻す判決を下した。 *ACLU v. Clapper*, <https://www.eff.org/document/acLU-v-clapper-second-circuit-opinion> 同条はかかる権限を授權していないとしたが、修正第四条違反の争点には判断を下していない。本件は安全保障とプライバシーのバランスをどうとるかの複雑な例の典型だとしている。 *Id.* at 96.

- (282) Samuel J. Rascoff, *Domesticating Intelligence*, 83 S. CAL. L. REV. 575 (2010).

- (283) *Id.* at 582. 「国内諜報は、行政国家を横断するさまざまな規制制度に慣れ親しんだ様相としての危険評価の一形態として、適切に認識される」。 *Id.* at 584.

- (284) *Id.* at 616. FISC Ct から令状を取って諜報を行う FISA のシステムは、公共の健康のような行政分野での行政上の令状を発給する十分に確立した実務に類推できるとする。 *Id.* at 640. ただ行政行為の司法審査と根本的に異なるのは、FISC Ct のそれは、審理は秘密であって、有意な対立主義 (adversarial) のプロセスをとっていないことである。 *Id.* at 642.

- (285) *Id.* at 605. 「国内の諜報は三つの重要な点で危険評価の一形態と考えられる。第一に、危険評価は将来的である。それは危害がなされる後ではなく、その前に危険評価を示すために危険を同定し、測る。第二に危険評価はアグレッシブである。社会での危険な実体や活動の蔓延を測るために広範なデータを探求する。第三に、危険評価はデータの慎重な科学的分析に依拠する」。 *Id.* at 605-6.

- (286) Sulmasy and Yoo, *supra* note 202 at 1236-37.

- (287) 二〇一三年九月に FBI 長官を辞めたロバート・モラーは、FBI として憲法の原則に忠実なことは個々の尋問や捜査よりも重要なのが原則だとしながらも、アメリカ市民をスパイする大統領権限の限界と常に緊張関係にあり、「テロとの戦い

には勝ったが、市民的自由は犠牲にした」とたたかれることだけは懸念していた。ティム・ワイナー／山田侑平訳『FBI 秘録 下』（文藝春秋、二〇一四年）三四二―三四三頁。なお同書は次の言葉で締めくくる。「原則が勝利を収める機会はある。危険の絶えないこの時代に、米国民が安全と自由の両方を確保できる可能性はまだ残っているのである」。同上書、三四三頁。

(288) Donohue, *supra* note 199 at 1203.

(289) See, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 439 (1974).

(290) 人権尊重や民主主義といった憲法的価値と諜報の効率性をはかるのに以下の五点を留意すべきと指摘される。1 公的な関心やプレッシャーを高める、2 文民の意識や能力を増大させる、3 透明性と効率性を支えるプロセスを制度化する、4 社会と諜報共同体のなかで、諜報の必要性を支持し信頼を高める政治文化を育成する、5 諜報活動を専門化させる。Steven C. Boraz and Thomas C. Bruneau, *Best Practices: Balancing Democracy and Effectiveness*, in BRUNEAU AND BORAZ, *supra* note 11 at 331, 333.

(291) Goldsmith, *supra* note 34 at 17.

(292) Balkin, *supra* note 4 at 19. 警察や社会保障の情報収集も同様であるとする。

(293) スノーデンが暴露したような状況では、国民はいつ諜報のターゲットにされるか不安である。そのため、修正第四条違反として事前にこうした諜報行為を差し止める訴訟が考えられる。最高裁は、FISAにはそうした訴権を認める規定がなく、個人の問題として争うには原告適格の要件を満たすべきところ、将来の損害 (future injury) は思弁的で原告適格がないとして、かかる訴訟を認めていない。Clapper v. Amnesty International, 133 S. Ct. 1138 (2013). FISAの電子的監視プログラムを司法権で解決させるには、原告適格が大きな壁となり、修正第四条で争うときは、個人の権利の損害という主観的な側面が強調されるから、なおやむを得ない。ANDREW NOLAN, FOREIGN SURVEILLANCE AND THE FUTURE OF STANDING TO SUE POST-CLAPPER, CRS REPORT FOR CONGRESS, July 10, 2013, at 13. See also, *id.* n.101.

(本学法学部兼任講師・首都大学東京法科大学院教授)